THE NEXT INTERFACE | R&D SCORECARD | VIRTUAL CASH

TECHNOLOGY REVIEW

DECEMBER 2001

WWW.TECHNOLOGYREVIEW.COM

SPECIAL REPORT

TECHNOLOGY VS. TERROR

FACE RECOGNITION, NEW DETECTORS FOR PATHOGENS, NETWORKED INFRASTRUCTURE AND ELECTRONIC SURVEILLANCE JOIN THE FRAY

USA $4.95 • CANADA $6.99

12 0 71658 01308 7

MIT'S MAGAZINE OF INNOVATION

THE LEXUS GS 430

Now we are not implying that the Lexus GS 430 is the perfect vehicle in which to achieve existential happiness.

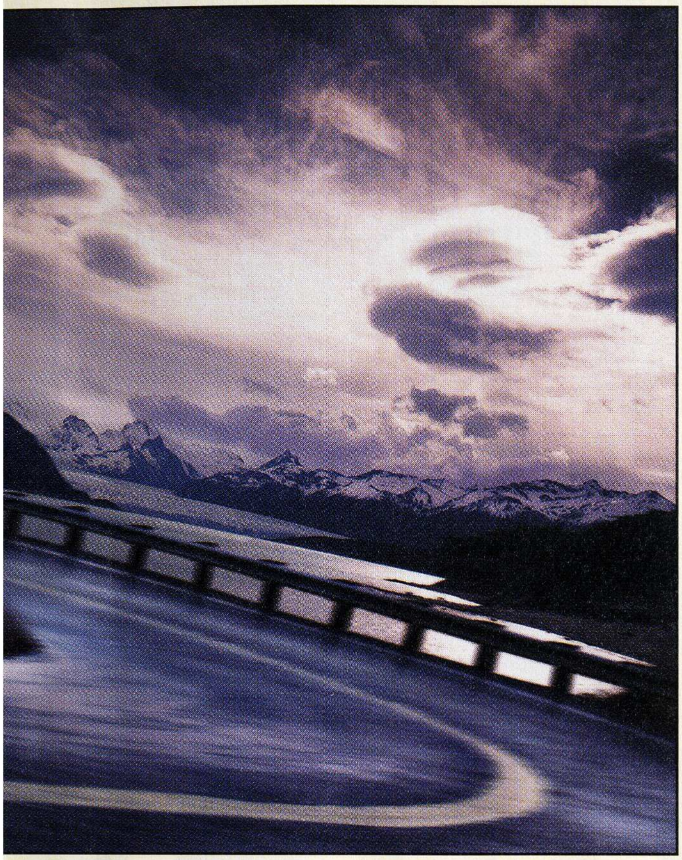
On the other hand, it is arguably one of the most balanced sport sedans ever made.

A cursory glance at the numbers is enough to awaken the most dour of souls: 4.3 liters, 32 valves, 300 horsepower and, remarkably, 325 pound-feet of torque.

ULTRA-LOW
EMISSIONS FOR
KARMA.
300 HORSEPOWER FOR
NIRVANA.

Such prodigious output is made possible by our aptly named Variable Valve Timing with intelligence (VVT-i for short) that increases response at low and medium rpm's. So when you punch the accelerator, things happen with a sense of urgency that you'll simply not experience elsewhere. Time compresses. Landscapes blur. Joy nears.

Perhaps more amazing than the sheer



power this car produces is the civility with which it is wielded. The GS 430 ride feels smooth and composed, while its handling borders on being telepathic.

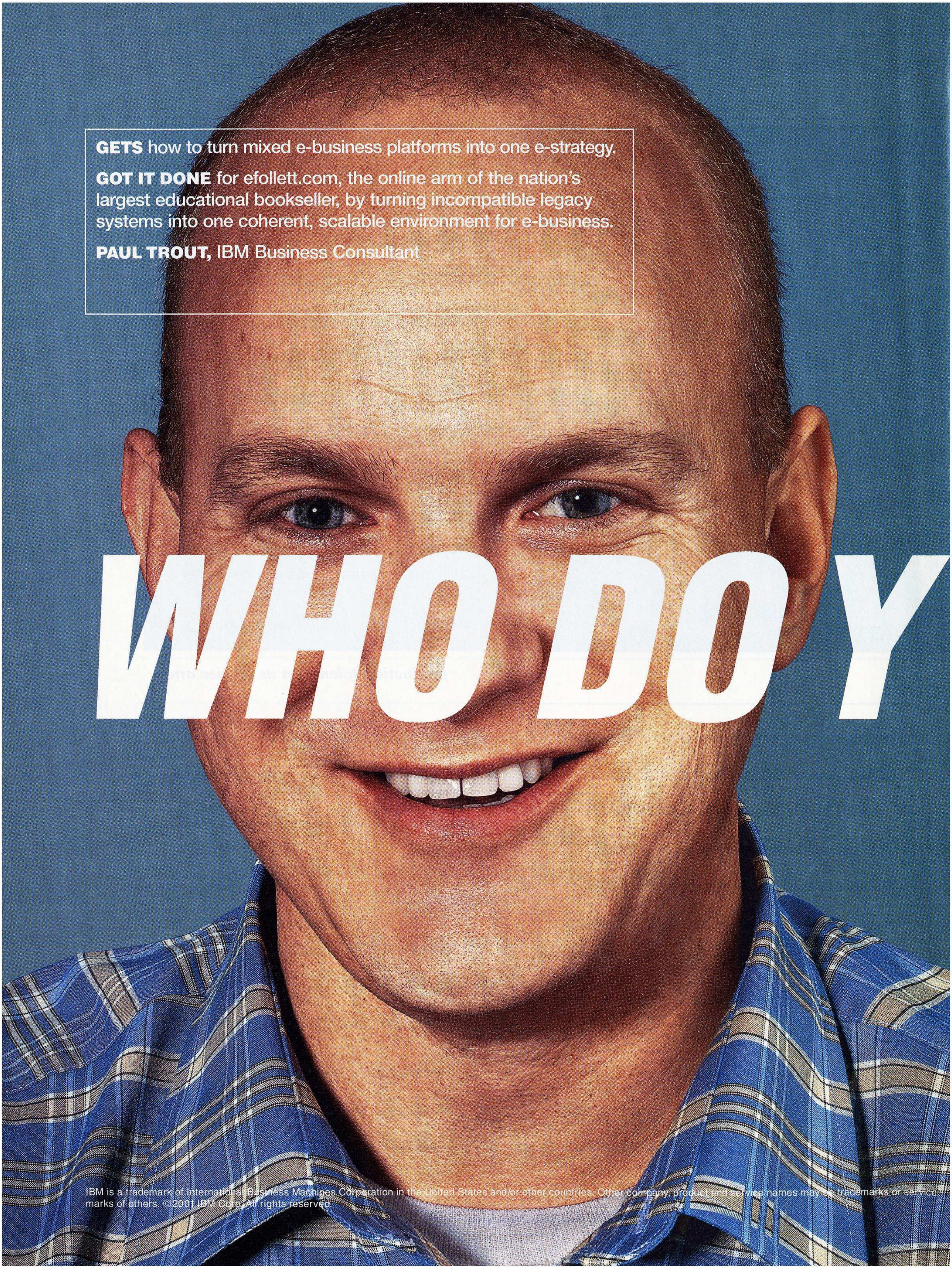
Interestingly enough, the same system providing this power is largely accountable for its rarefied U-LEV* status.

What good, after all, is creating one of the most exhilarating cars on the planet if there's no planet left to drive on?

So what on earth is U-LEV? Ultra-Low Emission Vehicle—a rating recognized by the EPA and the California Air Resources Board with the intent of reducing harmful emissions. In order to achieve this government rating, an automobile must emit one-third less harmful emissions than the average new car being sold today. How did Lexus engineer this masterstroke? An ingenious catalytic converter design. Unique induction technology. And production tolerances as precise and tight as you could possibly imagine. The end result of all of this innovation and technology is a powerful engine that runs exceptionally cleanly and efficiently. Because at Lexus, we firmly believe that a true performance automobile should not only be driven responsibly, it should be built responsibly, too.

Can an automobile delight, comfort, fascinate and energize you? Take lexus.com for a test drive. The Passionate Pursuit of Perfection.

LEXUS

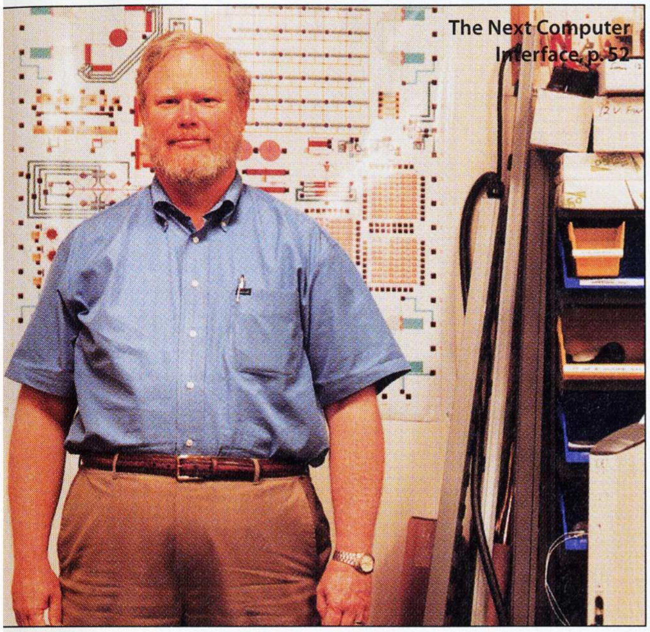

GETS how to turn mixed e-business platforms into one e-strategy.
GOT IT DONE for efollett.com, the online arm of the nation's largest educational bookseller, by turning incompatible legacy systems into one coherent, scalable environment for e-business.
PAUL TROUT, IBM Business Consultant
WHO DO Y
IBM is a trademark of International Business Machines Corporation in the United States and/or other countries. Other company, product and service names may be trademarks or service marks of others. ©2001 IBM Corp. All rights reserved.

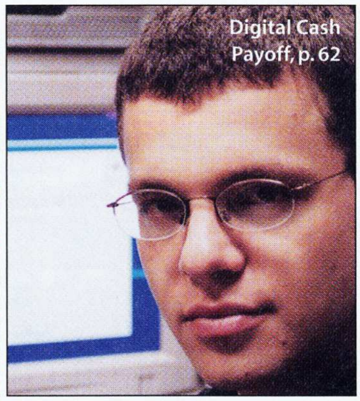

GETS how to speed up the wheels of the tractor business.
GOT IT DONE for John Deere by building an extranet that enables 10,000 JD dealers to place and track parts orders via the Web—reducing cycle time and cutting customer service costs by 30%.
BEA ELBERT, IBM Software Account Manager
OU NEED?
IBM
PEOPLE WHO GET IT. PEOPLE WHO GET IT DONE.
ibm.com/e-business/people

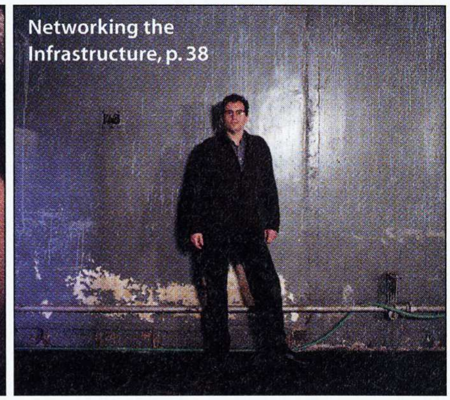
CONTENTS

FEATURES

TECHNOLOGY REVIEW VOLUME 104, NUMBER 10



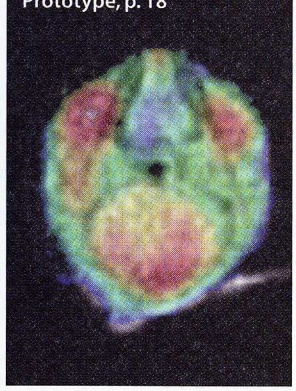


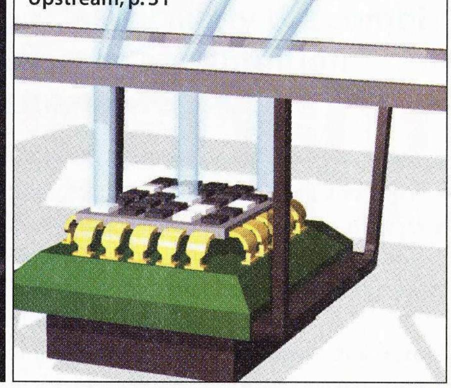


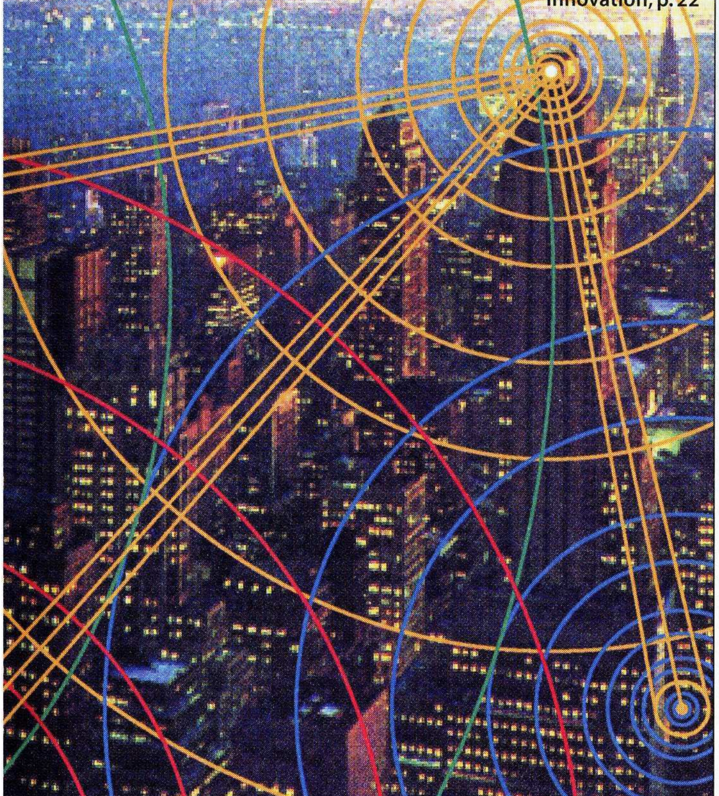
December 2001

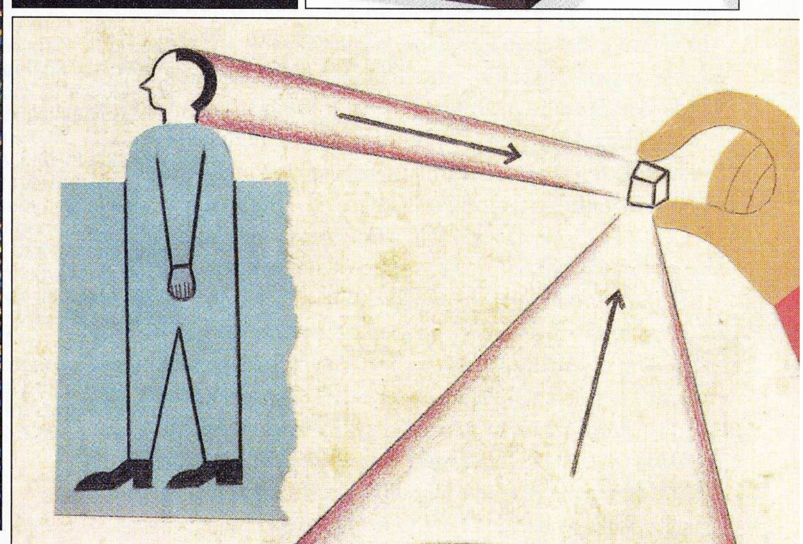
SPECIAL SECTION: TECHNOLOGY VS. TERROR

CONTENTS


Prototype, p. 18


Upstream, p. 31


Innovation, p. 22


Hawley, p. 86

WORLDCOM

today's business thought:

what's the best use of your company's time and money?

hint: it isn't managing IT infrastructure.

You have a business to run. And building and operating communications infrastructure probably isn't your core competency. So why devote your precious resources trying to reinvent the data networks, scalability, security and performance WorldCom is known for across the globe? After all, communications is *our* core business.

WorldCom has a team of experts whose sole focus is providing optimal solutions that are cost effective for your business. We manage those solutions through our global data centers, which plug directly into the world's farthest-reaching* IP network. Maybe that's why over 50% of the Fortune 1000 and their subsidiaries tap into WorldCom for complex IP services. Why not join them?

In these economic times, or really at any time, you can't afford to divert your attention away from driving your business. But you can afford WorldCom, and we're just a call away.

Visit www.worldcom.com/us/info/outsource or call 1-888-886-3829 for dozens of outsourcing solutions.

generation d.

* Based on global PoPs.

TECHNOLOGY VS. TERROR

Since we relaunched *Technology Review* in mid-1998, we've taken as our mission telling you about the most important emerging technologies and their potential impact on our society, economy, culture and individual lives. Most of the time, fulfilling that mission means talking about the remarkable transformative power of new technologies. We live at a time when three simultaneous technology revolutions are under way—in information technology, biotechnology and, just over the horizon, nanotechnology. What's more, those three revolutions will ultimately merge into a single force capable of changing almost everything about what it means to be human. As a result, writing and reporting for *Technology Review* is, most of the time, a pretty upbeat job.

Not always, though. One reason is that if our mission is to delineate the impact of emerging technologies, implicit in that mission is a responsibility to spell out the limits of those technologies—what they can't do now and won't be able to do in the future as far as we can see into it. We're intrigued by the power of new technologies, but we're not true believers in them. We aim to be just as hardheaded as we can. And the responsibility to be skeptical is never more important than when the stakes are high, when what's at issue isn't just economic or cultural change but the safety of our friends and family and neighbors. In the special report that forms the heart of this issue of *Technology Review*, "Technology vs. Terror," we've tried to give you a clear picture of just what it is that technology can do to help make us safer—along with what it can't do.

The essential message of this group of stories is conveyed in a memorable phrase from the essay by Edward Tenner *(p. 50)*. Tenner, a visiting researcher at Princeton and a widely published writer on technology, has twisted a cliché to tell us that what September 11 really brought home was "the shock of the old." Most of our military and intelligence agencies, he argues, were peering into the future, into a world where wars are virtual and the battlefield is cyberspace rather than deserts or mountains. All wrong, says Tenner—but not surprising. Every generation of technologists is in danger of forgetting the skills treasured by previous generations. Many young doctors, for instance, are wizards at interpreting batteries of high-tech diagnostic tests but aren't very skilled at using a stethoscope. Against such a background, it seems logical that the FBI and the CIA were glued to their computer screens while the terrorists were commandeering airliners armed with box cutters.

What good is technology, then, at protecting us? The answer, as four feature articles show, is that technology is valuable in sensing terrorist attacks of all kinds and in making our built environment more resistant to destruction. Dave Talbot's story, "Detecting Bioterrorism" *(p. 34)*, details efforts to create information networks to alert public-health authorities quickly to biological attacks. Indeed, a prototype version of this system was deployed at the inauguration of George W. Bush, where it detected, well, a flu outbreak.

The attacks of September 11 have also focused attention on the vulnerability of the large, complex systems on which our existence depends. In "Networking the Infrastructure" *(p. 38)*, Wade Roush shows that engineers are making systems such as the electric power grid harder to paralyze. Building on work that is already in motion to address difficulties in power delivery, power engineers will soon be able to give the power grid some of the capacity the Internet has to continue functioning even when part of the network has been taken down.

But if technology is becoming quite good at hardening major systems and alerting us when an attack has taken place, it still isn't good at alerting us to attacks before they take place and helping us to prevent them. One reason is that the freedom and abundance of electronic communication make it virtually impossible to exploit as an early-warning system. As Kevin Hogan tells us in "Can Spyware Work?" *(p. 43)*, several classified projects aimed at collecting and deciphering e-mail and voice traffic failed miserably in giving police or intelligence agencies a heads up before September 11. The reason is simple: the software for making sense of the traffic can't keep up with the volume. Don't expect that to change anytime soon.

Cutting-edge technology alone can't make us safe. Human factors are far more important, particularly the combination of experience and intuition known as "tacit knowledge."

Nor will high-tech methods of identifying suspected terrorists be of much help in the immediate future. In "Recognizing the Enemy" *(p. 48)*, Alexandra Stikeman describes a universal system of automatic personal identification that might one day emerge from the nascent field of face recognition. But that dream—instantaneous recognition of individuals through video surveillance—remains a fantasy. Rendering it effective would require a shared database of photos, presupposing a level of cooperation among officials that doesn't yet exist.

Fantasy isn't what we need now. In the foreseeable future the job of prevention will continue to depend on what Edward Tenner calls the "tacit knowledge" possessed by police and intelligence officers. Another way of putting it is intuition based on experience. That's what the Israeli airline El Al relies on. El Al, clearly an alluring target for terrorist groups throughout the Middle East, has an excellent safety record. A major reason is that the airline relies heavily on a combination of profiling and the intuition of well-trained security agents screening passengers at the gate. Pretty low tech. Then again, so are box cutters. *—John Benditt*

MIT'S MAGAZINE OF INNOVATION
TECHNOLOGY REVIEW

CUSTOMER SERVICE/SUBSCRIPTION INQUIRIES
NATIONAL: 800-877-5230
INTERNATIONAL: 386-447-6352
www.technologyreview.com/custserv/inquiry
Cost $34 per year
Canada residents add $10
Other foreign countries add $30

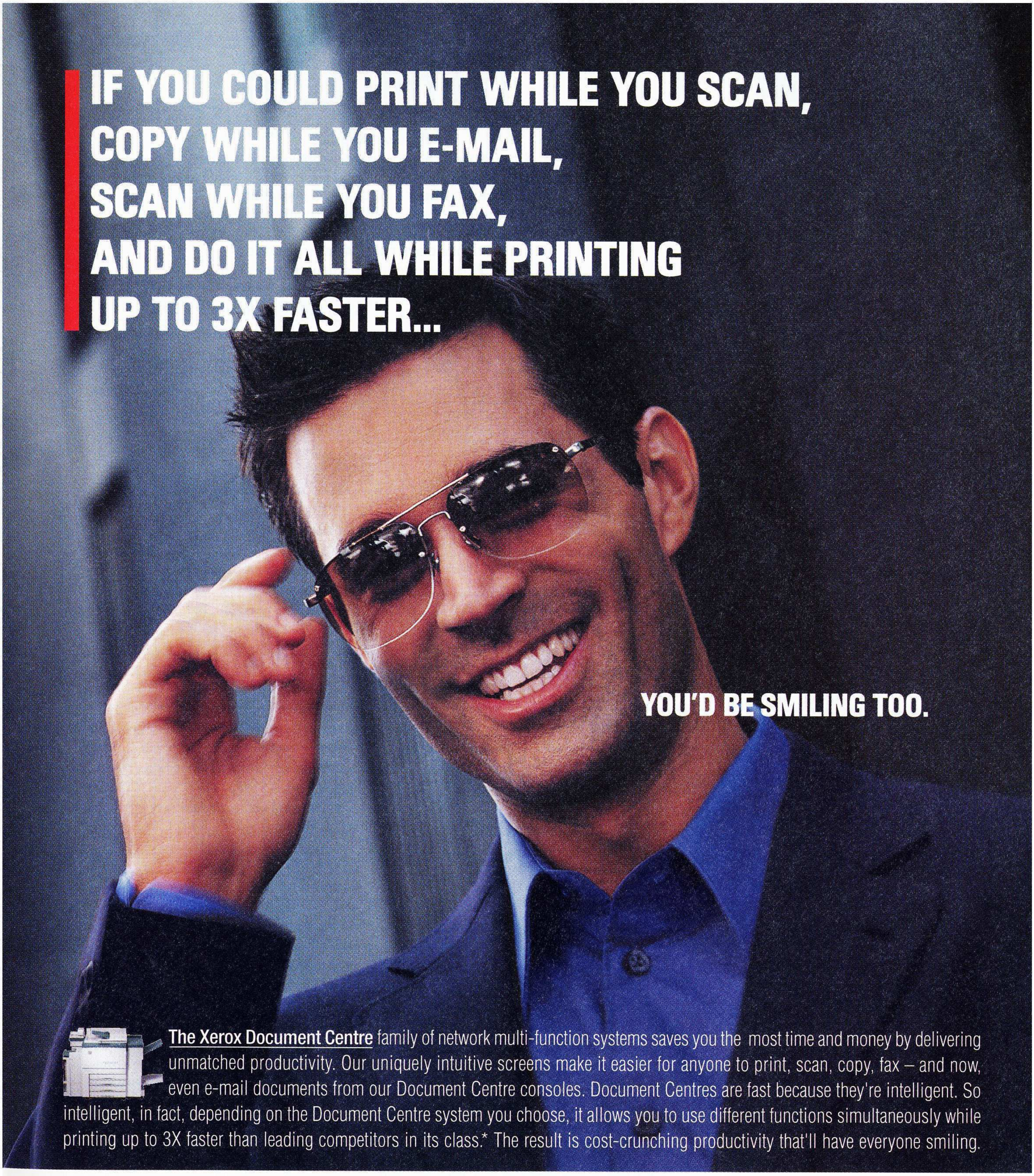
ADDRESS CHANGES
www.technologyreview.com/custserv/addresschange
MIT Records 617-253-8270 (Alums only)

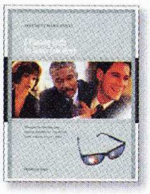
PERMISSIONS
978-750-8400
www.technologyreview.com/magazine/permissions.asp

REPRINTS
717-399-1900
sales@rmsreprints.com or
www.technologyreview.com/magazine/reprints.asp

TR RELAUNCH FUND
MILLENNIAL PATRON
Robert M. Metcalfe
CENTENNIAL PATRONS
Steve Kirsch
DuWayne J. Peterson Jr.

TECHNOLOGY REVIEW
One Main Street, 7th Floor
Cambridge MA 02142
TEL: 617-475-8000 FAX: 617-475-8043
www.technologyreview.com





SMILE. NOW YOU CAN LEARN HOW TO LOWER COSTS AND TAKE YOUR OFFICE PRODUCTIVITY TO THE NEXT LEVEL WITH OUR FREE "PLANNING GUIDE FOR SENIOR EXECUTIVES." TO GET YOURS, CALL 1 800 ASK XEROX, EXT. 369 OR VISIT WWW.XEROX.COM/SMILE

THE DOCUMENT COMPANY

XEROX

*Based upon independent testing versus leading competitive products conducted by BERTL (Digital Test Lab). Reports dated February, 2001. XEROX,® The Document Company® and Document Centre® are trademarks of XEROX CORPORATION. These models may contain some recycled components that are reconditioned.

United States Postal Service

Statement of Ownership, Management, and Circulation

1. Publication Title	2. Publication Number	3. Filing Date
Technology Review	5 3 5 - 9 4 0	10/1/01
4. Issue Frequency	5. Number of Issues Published Annually	6. Annual Subscription Price
Monthly	10	34.00

7. Complete Mailing Address of Known Office of Publication (Not printer) (Street, city, county, state, and ZIP+4)
MIT, 77 Massachusetts Ave, Middlesex, Cambridge, MA 02139
Contact Person: Corrine Callahan
Telephone: 617-475-8016

8. Complete Mailing Address of Headquarters or General Business Office of Publisher (Not printer)
MIT, 77 Massachusetts Ave, Cambridge, MA 02139

9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor (Do not leave blank)
Publisher (Name and complete mailing address)
R. Bruce Journey
MIT, 77 Massachusetts Ave, Cambridge, MA 02139
Editor (Name and complete mailing address)
John Benditt
MIT, 77 Massachusetts Ave, Cambridge, MA 02139
Managing Editor (Name and complete mailing address)
Tracy Staedter
MIT, 77 Massachusetts Ave, Cambridge, MA 02139

10. Owner (Do not leave blank. If the publication is owned by a corporation, give the name and address of the corporation immediately followed by the names and addresses of all stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, give the names and addresses of the individual owners. If owned by a partnership or other unincorporated firm, give its name and address as well as those of each individual owner. If the publication is published by a nonprofit organization, give its name and address.)

Full Name	Complete Mailing Address
Massachusetts Institute of	77 Massachusetts Ave.
Technology	Cambridge, MA 02139

11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities. If none, check box ▶ ☐ None

Full Name	Complete Mailing Address

12. Tax Status (For completion by nonprofit organizations authorized to mail at nonprofit rates) (Check one)
The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes:
☐ Has Not Changed During Preceding 12 Months
☐ Has Changed During Preceding 12 Months (Publisher must submit explanation of change with this statement)

PS Form 3526, October 1999 (See Instructions on Reverse)

13. Publication Title: Technology Review
14. Issue Date for Circulation Data Below: July/Aug 01

15. Extent and Nature of Circulation	Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Total Number of Copies (Net press run)	357,370	383,449
b. Paid and/or Requested Circulation (1) Paid/Requested Outside-County Mail Subscriptions Stated on Form 3541 (Include advertiser's proof and exchange copies)	272,880	303,282
(2) Paid In-County Subscriptions Stated on Form 3541 (Include advertiser's proof and exchange copies)	0	0
(3) Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Non-USPS Paid Distribution	26,790	30,771
(4) Other Classes Mailed Through the USPS	0	0
c. Total Paid and/or Requested Circulation [Sum of 15b. (1), (2),(3),and (4)]	299,669	334,053
d. Free Distribution by Mail (Samples, complimentary, and other free) (1) Outside-County as Stated on Form 3541	4,931	5,031
(2) In-County as Stated on Form 3541	0	0
(3) Other Classes Mailed Through the USPS	0	0
e. Free Distribution Outside the Mail (Carriers or other means)	2,225	0
f. Total Free Distribution (Sum of 15d. and 15e.)	7,156	5,031
g. Total Distribution (Sum of 15c. and 15f)	306,825	339,u84
h. Copies not Distributed	50,545	44,365
i. Total (Sum of 15g. and h.)	357,370	383,449
j. Percent Paid and/or Requested Circulation (15c. divided by 15g. times 100)	97.67	98.52

16. Publication of Statement of Ownership
☐ Publication required. Will be printed in the ______ issue of this publication. ☐ Publication not required.

17. Signature and Title of Editor, Publisher, Business Manager, or Owner
R. Bruce Journey Publisher, CEO
Date: 10/26/01

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including civil penalties).

Instructions to Publishers

1. Complete and file one copy of this form with your postmaster annually on or before October 1. Keep a copy of the completed form for your records.
2. In cases where the stockholder or security holder is a trustee, include in items 10 and 11 the name of the person or corporation for whom the trustee is acting. Also include the names and addresses of individuals who are stockholders who own or hold 1 percent or more of the total amount of bonds, mortgages, or other securities of the publishing corporation. In item 11, if none, check the box. Use blank sheets if more space is required.
3. Be sure to furnish all circulation information called for in item 15. Free circulation must be shown in items 15d, e, and f.
4. Item 15h., Copies not Distributed, must include (1) newsstand copies originally stated on Form 3541, and returned to the publisher, (2) estimated returns from news agents, and (3), copies for office use, leftovers, spoiled, and all other copies not distributed.
5. If the publication had Periodicals authorization as a general or requester publication, this Statement of Ownership, Management, and Circulation must be published; it must be printed in any issue in October or, if the publication is not published during October, the first issue printed after October.
6. In item 16, indicate the date of the issue in which this Statement of Ownership will be published.
7. Item 17 must be signed.

Failure to file or publish a statement of ownership may lead to suspension of Periodicals authorization.

PS Form 3526, October 1999 (Reverse)

MIT'S MAGAZINE OF INNOVATION

TECHNOLOGY REVIEW

PUBLISHER AND CEO
R. Bruce Journey, bruce.journey@technologyreview.com

VICE PRESIDENT AND GENERAL MANAGER
Martha Connors, martha.connors@technologyreview.com

VICE PRESIDENT, SALES AND MARKETING
Kate Dobson, kate.dobson@technologyreview.com

CORPORATE

BUSINESS DEVELOPMENT MANAGER
J. R. "Matt" Mattox
matt.mattox@technologyreview.com

HUMAN RESOURCES MANAGER
Ann E. Warner

DIRECTOR OF INFORMATION TECHNOLOGY
Lon Anderson

NETWORK COORDINATOR
Scott Hendry

DATABASE ADMINISTRATOR
Melissa Yu

TECHNICAL COORDINATOR
Chris Farwell

ASSISTANT TO THE VP/GM
Kimberly Pichi

EXECUTIVE ASSISTANT TO THE CEO
Kelli Talbot

OFFICE ADMINISTRATOR
Eileen Cahalane

SALES AND MARKETING

ASSISTANT TO THE VP, SALES AND MARKETING
Sharon Morani

ADVERTISING SERVICES COORDINATOR
Amy McLellan
amy.mclellan@technologyreview.com

MARKETING DIRECTOR
Marcy Dill

RESEARCH MANAGER
Kathleen Kennedy

MARKETING COMMUNICATIONS MANAGER
Rachel Valente

MARKETING COORDINATOR
Lisa Sperduto

TECHNOLOGYREVIEW.COM

VICE PRESIDENT AND GENERAL MANAGER
Martha Connors
martha.connors@technologyreview.com

DIRECTOR OF ONLINE SALES AND MARKETING
Brian Shepherd

STAFF EDITORS
David Cameron
Alan Leo

GRAPHIC DESIGNER
Matthew Bouchard

CONTENT MANAGER
Kristy Robinson

INTERNET OPERATIONS MANAGER
Christopher Pisano

CONTENT AND TRAFFIC ANALYST
Thomas Pimental

CONSUMER MARKETING

DIRECTOR OF CONSUMER MARKETING
Elaine Spencer

ASSOCIATE CONSUMER MARKETING DIRECTOR
Corrine L. Callahan

CONSUMER MARKETING PROMOTIONS MANAGER
Karen Lurie

CONSUMER MARKETING ASSOCIATE
Ian Milgram

FINANCE

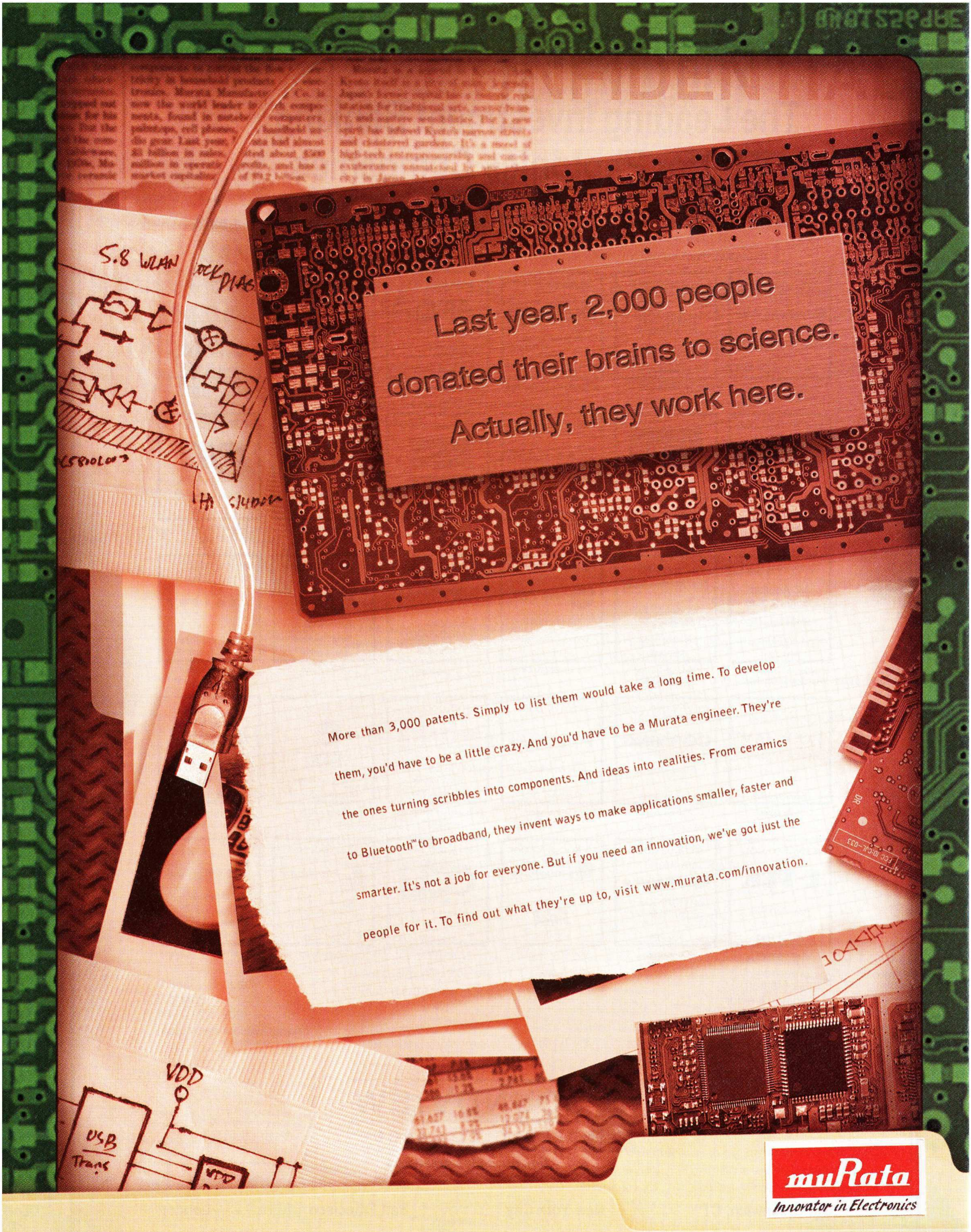
CONTROLLER
John W. Keegan

SENIOR ACCOUNTANT
John F. Leahy

ACCOUNTANT
Letitia Trecartin

ADVERTISING SALES

NEW ENGLAND/BOSTON: 617-475-8004	Paul Gillespie	paul.gillespie@technologyreview.com
MID-ATLANTIC/NEW YORK: 212-983-0011	Alan Levine	alan.levine@technologyreview.com
	Mason Wells	mason.wells@technologyreview.com
	Jamie Casale	jamie.casale@technologyreview.com
SOUTHEAST/NEW YORK: 212-983-0011	Dean Grant	dean.grant@technologyreview.com
SOUTHWEST/DALLAS: 972-625-6688	Randy Artcher	randy.artcher@tierney.com
	Steve Tierney	steve.tierney@tierney.com
MICHIGAN/DETROIT: 248-546-2222	Colleen Maiorana	colleenm@maiorana-partners.com
MIDWEST/CHICAGO: 312-629-5230	Penny Nasir	penny_nasir@worthmedia.com
	Chris Streuli	amsstreuli@aol.com
NORTHWEST/SAN FRANCISCO: 415-421-2999	Sarah L. Gammill	sarah.gammill@technologyreview.com
	Merrick Musolf	merrick.musolf@technologyreview.com
	Sam Staley	sam.staley@technologyreview.com
SOUTHERN CALIFORNIA/LA: 310-451-5655	Gregory Schipper	gschipper@whiteassociates.com
EUROPE: 44-207-630-0978	Anthony Fitzgerald	afitzgerald@mediamedia.co.uk
	David Wright	dwright@mediamedia.co.uk


Last year, 2,000 people
donated their brains to science.
Actually, they work here.
More than 3,000 patents. Simply to list them would take a long time. To develop them, you'd have to be a little crazy. And you'd have to be a Murata engineer. They're the ones turning scribbles into components. And ideas into realities. From ceramics to Bluetooth™ to broadband, they invent ways to make applications smaller, faster and smarter. It's not a job for everyone. But if you need an innovation, we've got just the people for it. To find out what they're up to, visit www.murata.com/innovation.
muRata
Innovator in Electronics
VDD
USB

FEEDBACK

LETTERS FROM OUR READERS

X MARKS THE SPOT

Simson Garfinkel makes a big mistake when he says "Microsoft innovates" ("Apple's X Factor," *TR* October 2001). Microsoft has never invented anything. It has bought out competitors, it has licensed technology from others, it has developed existing ideas, but it has not come up with anything really new since MS-DOS. At the time of the Microsoft antitrust trial, the optical mouse was being lauded as an example of Microsoft's innovation. From my understanding, this was a Hewlett-Packard innovation that Microsoft took over development of. The PC tablet, which is a pager, personal digital assistant and notebook all in one, has been cited as a possibility, but Apple Computer's R&D crew came up with a prototype casing design for something similar around 1998 or 1999 when Apple was trying to figure out where to take the laptop or the handheld computer next.

Yuri Shukost
Canberra, Australia

I read Simson Garfinkel's column with much interest. As a business owner with both Mac and Windows computers, I find it hard to keep up with all the frequent upgrades. We upgrade as needed and try to stay away from letting technology run our business as well as our thinking. Currently, we find ourselves at a crossroads: to upgrade or not to upgrade.

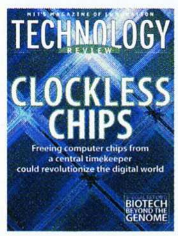
I wish Mr. Garfinkel would have elaborated more on how existing Macintosh software will run under OS X. It is well known that users of MacOS are incredibly loyal. So while OS X might be a mongrel, there are many who welcome a change that is actually not considered just another upgrade.

Lupe Alonzo
Richardson, TX

Simson Garfinkel's column was generally a fair and open-minded review of both the history of Apple and the importance of OS X. However, his statement that most of Apple's innovations have been in hardware is semi-incorrect. Although Apple has made great strides in hardware, it also creates wonderful software products.

For instance, there is QuickTime, the first high-quality digital media format for personal computers, which Apple started developing in the late 1980s. Other important Apple software products include the user-friendly video-editing-and-production programs such as iMovie, and the first consumer DVD creation software in iDVD and DVD Studio Pro. Also, don't forget iTunes, OS X Server (which provides an easy Web streaming and networking experience), AppleWorks, ColorSync (professional color management for the publishing industry), and WebObjects (Apple's object-oriented program that allows webmasters to quickly develop and deploy Web and Java applications).

Jonathan Parker
King of Prussia, PA



"Users of MacOS are incredibly loyal. So while OS X might be a mongrel, there are many who welcome a change that is actually not considered just another upgrade."

Simson Garfinkel responds:
It's true that Apple has published a lot of software over the past two decades. But two of the products that Parker mentions—OS X Server and WebObjects—were largely developed by NeXT, not Apple. ITunes is a clone of MusicMatch's product. QuickTime was certainly innovative, but it has a hard time competing against the media players developed by RealNetworks and Microsoft. Also, since Apple's software is offered only for Apple computers and not for other platforms, it looks to me as if the main purpose of Apple's software is to help sell Apple hardware. Innovative software should be able to stand on its own.

CONTACT US

WRITE: ***Technology Review*, One Main Street, 7th Floor, Cambridge MA 02142**
FAX: 617-475-8043
E-MAIL: letters@technologyreview.com

- **Please include your address, telephone number and e-mail address.**
- **To participate in our online forums, visit www.technologyreview.com and click on "Forums," in the menu at left.**
- **Letters may be edited for clarity and length.**

STOP THE CLOCKS

Claire Tristram's story "It's Time for Clockless Chips" (*TR* October 2001) would lead one to conclude that commercial computers never had asynchronous technology. The timeline accompanying the piece states that during the 1960s, "the idea of clockless chips all but disappeared, kept alive only by a few esoteric papers from academics." This is not true.

I was codesigner with Gordon Bell of the PDP-6, a large commercial computer built and sold by Digital Equipment in 1964 and 1965. It employed discrete-transistor asynchronous logic in two ways. First, most logic functions proceeded based on timing individually determined by circuit analysis of how long would be needed; there was no central clock. Second, the arithmetic unit was truly "asynchronous" and "clockless." "Handshake" signals detected when the operation was completed, and allowed other processing to proceed, just as shown in the illustration accompanying your article.

Alan Kotok
World Wide Web Consortium
Cambridge, MA

FEEDBACK

Your story on clockless computing stated that asynchronous processing was of only academic interest in the early days of computing. I wrote my first computer program on an asynchronous Philco 2000 computer. It was a transistorized mainframe that was, for a few years, probably the fastest computer in the world for scientific computation. Its customers included the North American Aerospace Defense Command, the U.S. Atomic Energy Commission and Ford Motor.

I believe the Philco 2000 missed being a major success primarily because Philco decided to ignore COBOL, the first widely used programming language for business applications. It instead implemented its own compiler for business processing. Philco also used one-inch tapes when the industry was adopting half-inch tapes. Such cavalier treatment of standards may be why Philco is occasionally remembered for radios and washing machines, and not for asynchronous computing.

Ron Bierman
San Diego, CA

I found it odd that an article on asynchronous logic design would make no mention of the fundamental synchronizing problem. When asynchronous signals converge at a flip-flop (the basic element of any register), there is a possibility of the circuit being nudged into a "metastable state," part way between one and zero. Once this happens, there is no limit to how long it may stay in that state. Imagine flipping a box cover through a 180-degree arc, between its open and closed states. Bad luck in timing would leave the cover balanced at 90 degrees, where it may hang for an indeterminate amount of time before falling one way or the other.

I've seen this problem bite engineers several times in my career; most hardware design engineers understand it poorly. One reason clocked designs are so appealing is that, for the most part, they eliminate this problem. But it

is an issue that asynchronous designers had better understand thoroughly.

Lawrence J. Krakauer
Wayland, MA

Claire Tristram responds:
Regarding successful asynchronous projects during the 1960s: with Digital Equipment no longer existing as a separate company and with Philco out of the computer business, it's a sad fact that many of these companies' innovations have been obscured by time. It is nevertheless true that in the 1960s, asynchronous research at universities all but died; the number of papers was negligible, picking up again only in the mid-1990s.

As for the suggestion that I should have included a more thorough explanation of the challenges faced by asynchronous-chip engineers, neither experts in the field of asynchronous design nor their critics interviewed for the story thought that the problem described by Mr. Krakauer was insurmountable.

ELEVATE TO LEVITATE

It is too bad that Tracy Staedter's piece on magnetically levitated trains ("Visualize," *TR* October 2001) did not credit the MIT professors who won the original patents on maglev technology, which was developed in the 1940s. For a fraction of the cost that it would take to build a maglev system between Baltimore and Washington, the entire electrification between New York and Washington could be modernized to accept such high-speed trains. But in highly populated areas, a maglev system has to be on an elevated structure for operational-safety reasons. The guideway has to be free of debris, animals and trash. And will the communities accept such parallel elevated structures, not to mention the fact that there have to be at least two tracks for bidirectional operation?

Gregory G. Gagarin
Chevy Chase, MD

Tracy Staedter responds:
MIT holds three patents for magnetic levitation technology, specifically for the integrated circuits that help keep the train afloat. But the basic idea dates back to before researchers at the Institute became involved. In the early 1900s, Robert Goddard—who is credited with inventing modern rocketry—conceived of electromagnetic roadbeds that would repel train cars without friction, and he published an editorial on the subject in *Scientific American* in 1909. In 1910, Emile Bachelet applied for a patent on his magnetically levitated rail technology, planned for use in a never-built mail delivery system.

With regard to your questions about society's acceptance of magnetic levitation as viable transportation, with any luck they will be answered after the U.S. Department of Transportation makes its choice about whether Pittsburgh or Baltimore and Washington will receive the $950 million to build the train.

THE BASICS

I was surprised to read Thomas Kurtz's comment on the legacy of the BASIC programming language, as described in "Trailing Edge" (*TR* October 2001): "Sorry to say, but I don't think we had much effect." I couldn't disagree more. I grew up without a computer or TV at home. Whenever my parents would take my sister and me to a store that had computers (Atari, Commodore, Tandy, Texas Instruments) on display, my sister and I would run to the electronics section and "program."

Using your programming language, Mr. Kurtz, we would set up counting loops and had races between machines. We'd set our names scrolling wildly across the screens. We eventually figured out how to control the machines' sound and color. Inspired by those simple moments, I've gone on to do many exciting things in the field of information technology. Was BASIC responsible for where I am today? Maybe, maybe not. But that's not the point. We always had a blast pounding out as much code as we could before mom and dad would call us to the check-out register. So thanks for BASIC!

Scott D. Szeglowski
Williamsville, NY

E-HEALTH

Excellent reasons exist why less than five percent of U.S. physicians use electronic medical records ("Electronic Medical Records," *TR* October 2001). Our clinic started using an electronic medical record system in June 2000. The results have been disheartening: physicians must spend two to 10 times longer charting in an electronic medical record than a paper one. The system requires multiple windows and clicks to perform simple tasks such as writing a prescription or ordering lab tests. More time spent charting means less time for patient care, research and teaching. Inputting lab data from outside laboratories also requires skilled personnel, which increases our expenses. Physicians' use of electronic medical records will remain low until their benefits exceed their problems.

John L. Kirkland
Endocrine and Metabolism Service
Texas Children's Hospital
Houston, TX

EDITOR'S NOTE:
"Bankrolling the Future"—a Q&A with Bob Metcalfe and Nobelist Walter Gilbert (*TR* October 2001)—should have noted that Metcalfe is on the board of *Technology Review* and made a substantial contribution to the magazine's relaunch fund.

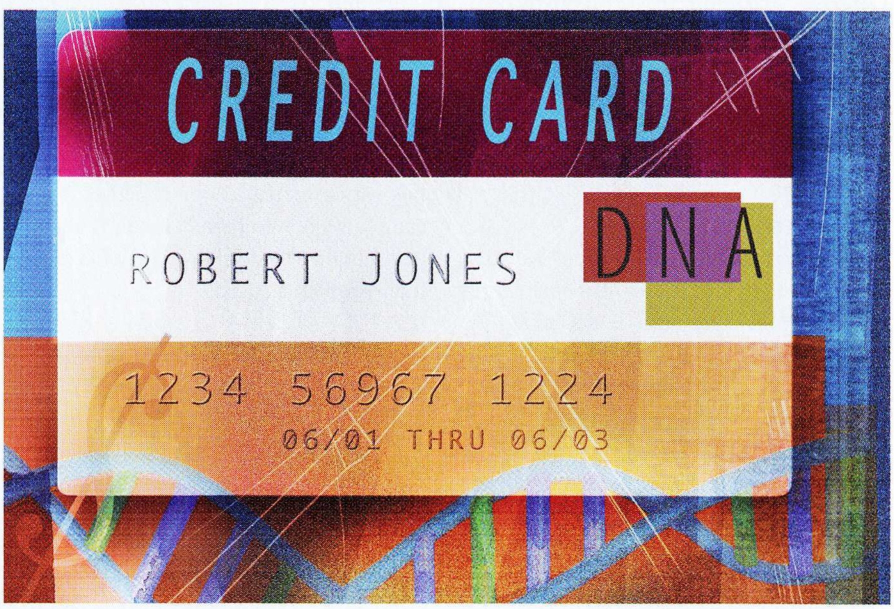
CORRECTION:
In the article "It's Time for Clockless Chips" (*TR* October 2001), Jo Ebergen was incorrectly identified in a second reference. Ebergen is an engineer at Sun Microsystems.

MOTORFOOT

Stroke victims and other people suffering from "drop foot"—a condition in which the front of the foot can't be controlled—generally wear stiff braces to keep their afflicted feet from flopping and dragging when they walk. But a device under development could give them a robotic boost for improved mobility. Instructor Hugh Herr and graduate student Joaquin Blaya of a joint MIT-Harvard program in health technology, together with electrical engineer Gill Pratt of Olin College in Needham, MA, built an ankle brace with a motor that raises and lowers the front of the foot as the heel strikes the ground and lifts again, providing more natural movement and a reduced risk of falling. The battery-powered device, developed at MIT's Artificial Intelligence Laboratory, uses algorithms modeled on "biological information about how a normal ankle is controlled," Herr says. The first tests of the contraption on real patients are expected to begin late this year.

PROGRAMMING OUT LOUD

Writing software by voice can be extremely tedious. Code that would take a few keystrokes to type must be spoken as lengthy word strings containing hyphens, slashes and barely pronounceable commands. Alain Désilets of the National Research Council of Canada in Ottawa is developing a software tool called VoiceCode that makes programming by voice a lot simpler. Instead of having to dictate tongue-twisting syntax, the programmer can use a simplified pseudocode. The software infers punctuation symbols from context, for example, liberating the programmer from having to utter every comma, bracket and semicolon. It automatically converts the pseudocode into working code in such common languages as C, C++ or Java. Désilets plans to begin distributing VoiceCode as a free, open-source application early in 2002.



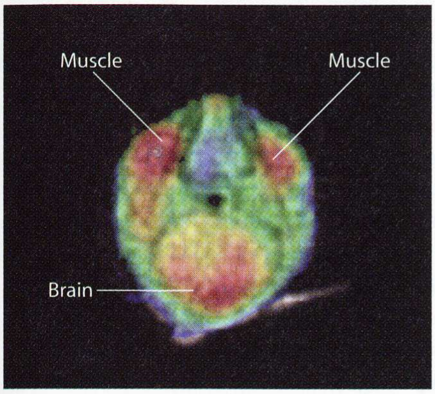
DNA ID

Every year, fake credit cards or pirated products like CDs cost businesses billions of dollars, and some offenders have discovered how to forge the holograms that many companies stick on products to prevent counterfeiting. Taiwan-based Biowell Technology has developed a way to authenticate consumer products, using the stuff that makes every living being one of a kind: DNA. Each of Biowell's millimeter-wide chips contains unique fragments of synthetic DNA. Manufacturers could embed the chips in their products; Biowell's proprietary reader sends a current into the chip, which emits a distinct signal caused by its interaction with the DNA. Each product could be matched with a specific type of DNA, and signals from an embedded chip would tell whether a product was authentic. With the vast number of possible sequences, the DNA would be extremely difficult to replicate. Biowell launched the chip in August and will soon ship to its first customer: an undisclosed Brazilian bank.

TRAVELER'S FRIEND

One of the challenges of traveling abroad is trying to make sense of signs and restaurant menus written in a foreign language. A translation device being developed at IBM's Almaden Research Center in San Jose, CA, could ease the alienation. Called InfoScope, the unit consists of a handheld device equipped with a digital camera that takes snapshots of the text the user is interested in. The image is sent wirelessly, via the user's cell phone, to a remote server. The server identifies what in the image is text, and then translates the words into a selected language. Within 15 seconds, the translation is relayed back to the handheld and superimposed on the photographed scene *(photo)*. IBM researcher Ismail Haritaoglu, InfoScope's chief architect, says the device could be on the market in two to five years.

PHOTOGRAPHS: IBM RESEARCH (TRANSLATOR); HUGH HERR (MOTORFOOT); ILLUSTRATION: VITO ALUIA



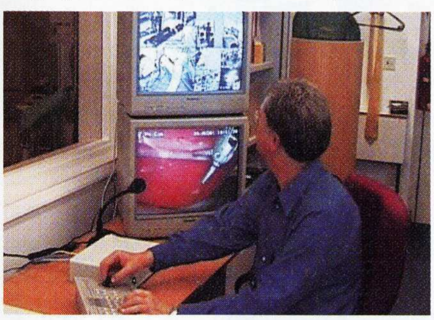
DOUBLE VISION

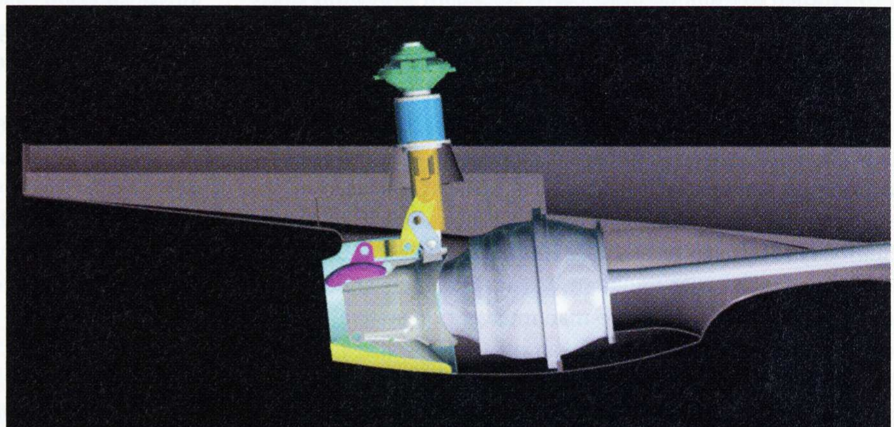
The two most vaunted medical-imaging technologies have led separate existences. Positron emission tomography (PET) provides snapshots of the human metabolism, while magnetic resonance imaging (MRI) captures high-resolution pictures of anatomical structures. MRI could pinpoint a tumor's location, for example, while PET revealed whether a drug was working to cut off its blood supply. Yet the two techniques have not been used simultaneously in humans; the metal inside the PET camera wreaks havoc with the MRI scanner's powerful magnet.

Researchers at King's College in London and the University of California, Davis, are working on a combination scanner that places a PET camera made of plastic and fiber optics inside an MRI magnet. They have built shoebox-size models that can image metabolic changes and anatomy simultaneously in the bodies of mice and rats *(the image at left is of a rat's head)* and hope to eventually build a prototype large enough for human testing.

SURGICAL BLACK BOX

A new data-recording system could pinpoint the causes of botched medical procedures. The system—modeled after a cockpit data recorder—records numerous aspects of a surgery for later review: patients' vital signs, spoken conversations and staff comings and goings. Sensors in the surgeon's gloves document his or her hand motions. The data recorder will help prevent future medical errors, says inventor Ara Darzi, professor of surgery at Imperial College in London. Darzi expects to transfer his patented prototype *(photo)* into an operating room next year and eventually to start a company to sell the system. Darzi admits his fellow doctors are "concerned about a recording of what they say during surgery—how many bad words they can use."





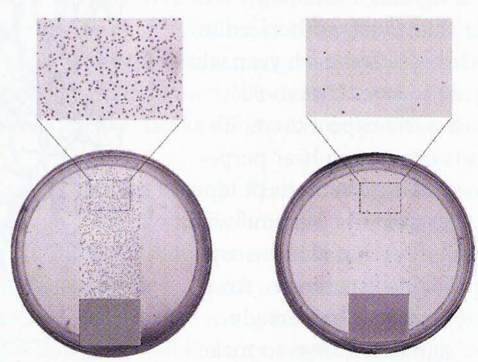
Cutaway of a waterjet that expels its propulsive stream beneath the surface to lower noise.

JET BOATS

Ships and even small boats are a major source of noise and other pollution, a growing concern along today's crowded coasts. One solution: a waterjet technology being developed by Rolls-Royce Naval Marine in Walpole, MA. The waterjets propel ships by shooting water out their sterns, allowing them to maneuver in water that would be too shallow for comparably sized vessels that rely on propellers and rudders. And unlike the waterjets used in personal watercraft and some ferries, which expel water above the vessels' waterlines, the new design discharges the propulsive stream underwater, thereby reducing wake and lowering noise. The Rolls-Royce waterjet operates at 30,000 to 50,000 horsepower—suitable for propelling fast ships like naval destroyers, which would benefit from the underwater jets' stealth. Smaller boats also may benefit from similar technology, though; a 2,000-horsepower version is scheduled for testing in spring 2003.

BACTERIA-BUSTING SURFACE

The age of chemical warfare against bacteria could soon end. Biologist Kim Lewis of Northeastern University and chemist Alexander Klibanov of MIT teamed up to create an environmentally friendly surface that stays sterile. The surface, which can be applied to virtually any material—including glass, metal, plastic or wood—consists of microscopic polymer bristles. Any bacterium landing on the surface is killed; the polymer spikes poke holes in the microbe's membrane, and the cell's contents squirt out. Although chemical biocides can create resistant bacteria, Lewis and Klibanov's technique attacks such a fundamental constituent of bacteria—the membrane—that species are unlikely to develop a defense against it. The researchers plan to start a company or partner with an existing one to develop the material. They foresee applications ranging from toys to public telephones to drinking-water pipes.



Bacteria (left) perish on sterile surface (right).

JOERG TILLER AND ALEXANDER M. KLIBANOV (SURFACE); IMPERIAL COLLEGE SCHOOL OF MEDICINE (BLACK BOX); ROLLS-ROYCE NAVAL MARINE (WATERJET); SIMON CHERRY UC DAVIS (PET/MRI SCAN)

HOW NOT TO FIGHT TERROR

Box cutters, some flight training and a lot of determination. Although it now seems clear that the hijackers of September 11 had the support of an international terror organization, the real lesson is that it is frighteningly easy for a small number of intelligent people, acting together, to do a tremendous amount of damage.

Technologists routinely underestimate the power of low-tech attacks. After all, it's much more interesting (and lucrative) to work on the Bush administration's national missile defense project than to think up practical strategies for protecting office buildings from fire, truck bombs and suicide pilots.

But even more disturbing than our failure to plan for the terrorist attack is the nature of our antiterrorist planning in the days that followed. Two days after the attacks, New Hampshire senator Judd Gregg called for a global ban on "uncrackable" encryption systems. Within a week, Attorney General John Ashcroft started arguing for a dramatic expansion in the FBI's authority to wiretap telephones; his proposed law would make such taps much easier to obtain. Meanwhile, there are calls to expand the use of the FBI's e-mail interception system, known as Carnivore, and the National Security Agency's Echelon surveillance system *(see "Can Spyware Work?" p. 43)*. Even a national identification card with ATM-like verification stations might be in the works.

Ashcroft and Bush want Congress to act fast; by the time you read this, their legislative agenda will be law. But even after Congress does as it is told, and even if the Supreme Court upholds the new laws as constitutional, America won't be a fundamentally safer place.

Let's look first at wiretapping, a tremendously powerful crime-fighting technology. With fewer than 2,000 authorized in the United States each year, wiretaps are so rare that crooks almost never expect them; it's not uncommon to hear perpetrators joking on intercept tapes that they should be careful with what they say because the cops are probably listening in. And the government has already taken significant steps to make wiretapping more effective. In 1994, Congress passed legislation that opened the world of digital telephony to the G-man's alligator clips. The law requires that every telephone switch sold in the United States be wiretap ready. It forces cell-phone companies to deploy equipment that exists solely for the purpose of intercepting phone conversations and sending an audio copy to the feds.

The wiretap laws still need some work. Back in 1995, for example, nobody imagined that drugstores would one day be selling disposable cell phones: it simply doesn't make sense to force the FBI to get a different wiretap order for every phone number that it wishes to bug. That's why the law was amended again to allow the use of "roving wiretaps." According to the U.S. government's own Wiretap Report, roving wiretaps were approved for seven federal investigations and 20 state investigations in 2000. (More than half of those cases were drug investigations; none of them were for terrorism.)

But even with such authority, and even if Ashcroft's expanded wiretap provisions had been in place in August 2001, it is doubtful that the September 11 attacks would have been anticipated, let alone prevented. And if we require the FBI to wiretap every phone call of every foreigner in the United

PETER HORVATH

States, it's doubtful that the agency will have the resources to even listen to all the tapes, let alone make sense of the often guarded language of people plotting crimes.

Nor is limiting the use of encryption the way to go. Listening to Senator Gregg's scary talk about terrorists using unbreakable encryption systems, it is hard to imagine any American contesting restrictions on such an inherently dangerous technology. Gregg and the FBI have long opposed strong encryption on the grounds it limits the ability to conduct searches and execute wiretaps. That's because in recent years, cops have been increasingly frustrated by encrypted files on seized computers in cases involving financial crimes, child pornography and drug dealing. To the FBI's vaunted Carnivore system, encrypted e-mail is, as they say, a cipher. And voice encryption can render a telephone wiretap useless.

But despite reports that Osama bin Laden is a big fan of encryption, a ban on tough encryption systems wouldn't have prevented the terrorist attacks of September 11. For starters, all the terrorists had to do to scramble their conversations was speak quickly in Dari or Pashto—two Afghan languages for which we have few translators available. This is not a new trick: in World War II, the U.S. military used Navajo "code talkers" speaking in their native language to create an unbreakable communications system.

Even if we could persuade our enemies to speak in English, there is nothing to prevent them from using strong encryption. After all, software that makes unbreakable codes has been available worldwide for more than a decade. Laws banning crypto will have no more effect than laws against flying fully fueled Boeing 767s into 100-story skyscrapers.

On the other hand, laws mandating the use of weakened encryption or "key escrow" could have a devastating impact on business and e-commerce. What Gregg and others fail to realize is that the vast majority of cryptography users today are not terrorists and drug dealers but U.S. businesses. Many banks and brokerage firms, for example, demand that their customers use an "unbreakable" encryption scheme based on a digital key 128 bits long when accessing electronic banking systems. Encryption likewise protects credit card numbers used to make purchases over the Internet. And a growing number of U.S. companies operating overseas use encryption to give branch offices secure links to the home office's computers. Over the last 10 years, corporations have experimented with weaker forms of encryption that include "back doors" for law enforcement. Their almost universal conclusion: the technology is too complex to deploy, and it creates risks and vulnerabilities that are unacceptable to many users.

The third infotech weapon commonly called upon to fight terrorists is a national ID card. But the United States already has a de facto national identity card: it's called a driver's license. Over the past 10 years, driver's licenses have been standardized, they have been equipped with bar codes and magnetic strips, and states have created databases of digitized driver's-license photographs. Indeed, a driver's license is the most readily accepted identification for anyone flying on an airplane, opening a bank account or obtaining most social services.

WEBB CHAPPELL

Adding biometric identifiers like fingerprints or face prints to the driver's license and requiring that it be carried at all times would not have prevented the September 11 attacks. Don't forget, Mohamed Atta and at least several other hijackers had valid driver's licenses. And while many of the attackers were using stolen identities, those identities were stolen overseas. If the United States had a biometrically enabled national identity card, the hijackers would have been issued those cards when they legally entered our country—under whatever names they had already stolen.

Even after Congress passes the Bush administration's proposed counterterrorism laws, and even if the Supreme Court upholds them as constitutional, America won't be a fundamentally safer place.

If we really want to ban technologies that have been used by international terrorists, we should start with box cutters: they are small, hard to detect and have a proven track record. Ceramic knives are equally stealthy and dangerous: better ban them too. While we're at it, we might as well ban commercial airliners: let's see those terrorists try to hijack a train!

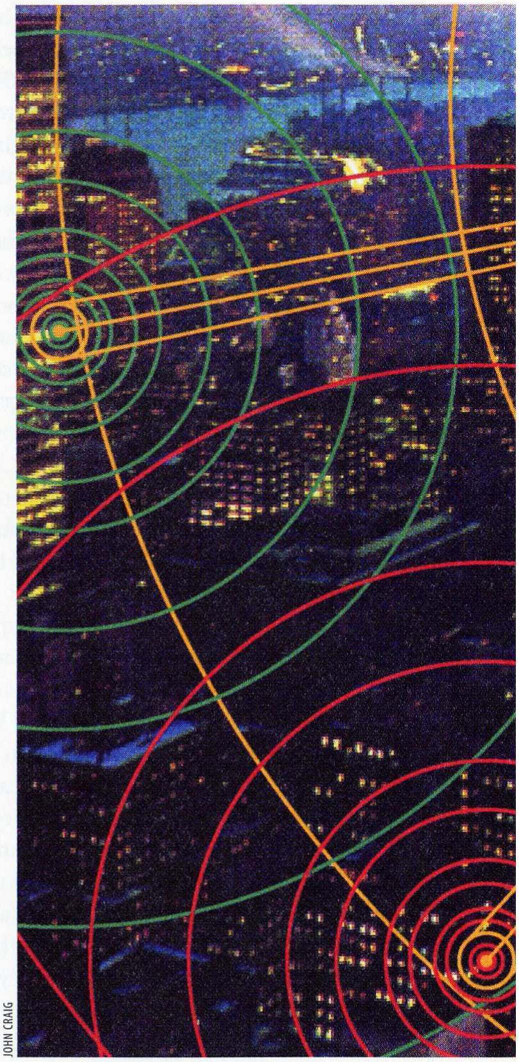
Banning additional carry-on items is not the way to go. Instead of loading the plane with five terrorists, next time the enemy might use 20. A contingent that large could take over the passenger cabin without any weapons whatsoever. That's why aviation experts are sensibly calling for stronger doors separating pilots from passenger cabins.

Meanwhile, we need to harden the rest of our society, because the next assault will almost certainly not involve the hijacking of a civilian airliner. Two weeks after the attacks in New York, the sight of small planes flying low over Massachusetts's Quabbin Reservoir, which supplies Boston's water, prompted fears that the reservoir might be poisoned. The Massachusetts Water Resources Authority dismissed such fears as baseless, saying that it performs 100 safety tests on the reservoir every week, and that in any event, Quabbin is too big to poison. This made me feel somewhat safe—until I learned that these weekly checks don't include tests for radioactivity.

We have the capacity to turn the United States into a surveillance society the likes of which the world has never seen. We could also significantly reduce the chances of a successful terrorist action in the future—a quite separate pursuit. It looks like Bush and Ashcroft are using September 11 as an excuse to clamp down on civil liberties, not as a wake-up call for solving these hard problems. TR

UNWIRING THE WEB

Community-owned wireless networks are gaining popularity—and could help bridge the digital divide.



JOHN CRAIG

It's an increasingly common scene: a telecommuter perched on a park bench, pecking away at a laptop. But a peek over her shoulder reveals a more startling sight: she's surfing the Web, outdoors and cable free.

Anywhere, anytime Internet access is gaining ground across the United States as wireless networks owned and run by their users spring up in more cities each month—25 at last count. Although companies like Texas-based Wayport and MobileStar have provided wireless access in places like hotels, airports and coffee shops, the new cooperatively run networks are, for the first time, allowing users to surf in outdoor public areas. These networks are set up by groups whose members lend out their Internet access by hooking high-speed digital subscriber line (DSL) or cable modem connections up to wireless base stations. These base stations transmit the bandwidth to any nearby computer—commonly a laptop or handheld—equipped with an antenna to receive the signal.

What began on the West Coast as "geek networks" set up mainly by computer professionals has taken a socially conscious turn in New York City. Urban researcher Anthony Townsend helped create NYCwireless, a volunteer organization, not just to provide wireless Internet access in New York's public spaces but also to bridge the digital divide, bringing broadband Internet access to poorer parts of the city. "A lot of the other groups are interested in building a network that's for themselves when they're outside the office or home," says Townsend. "We're trying to build a public service."

Townsend cofounded NYCwireless earlier this year after some Boston-area friends tried to set up a wireless network for a more mundane reason: they couldn't get high-speed Internet access in their neighborhoods. He found that the same was true in many areas of New York, especially low-income areas, where he asserts cable and telephone companies have not upgraded their infrastructure to bring in broadband access. While Verizon, for instance, says DSL service is available in every area of Manhattan, NYCwireless's mapping has shown the service's coverage is not nearly as extensive in Harlem as in other neighborhoods.

NYCwireless is trying to create formal relationships with organizations that control public spaces; it has begun providing Internet access in public areas by establishing ten wireless access points around the city and one in Hoboken, NJ, and is talking with Amtrak about bringing access to Penn Station. And NYCwireless started its efforts to bridge the digital divide by submitting an Urban Empowerment Zone grant application, along with other area groups, to provide wireless broadband access to housing projects and other buildings in Yonkers, just north of New York City. The organization also has plans to gather financial and equipment donations to provide low-income residents with computers that can access the networks.

Community-based wireless networks date back at least to 1996, when Sun Microsystems set an experimental one up in Aspen, CO. But it wasn't until Apple Computer popularized the 802.11b wireless networking standard—or "Wi-Fi"—with its AirPort wireless base stations that the idea caught on. "Apple was really the company that started it," says Nigel Ballard, a wireless consultant involved in Portland, OR's Personal Telco community network. "Up until then, it was just too expensive for consumers." Since then, community-owned wireless networks have emerged nationwide, each with slightly different motives and methods.

So far, only NYCwireless has set out with overtly altruistic aims. Most of the wireless groups have what Barrett Canon, founder of a Houston-area network, describes as selfish motives: "We just wanted to be able to get on the Net wherever we are." Others want to bridge "the last mile"—bringing high-speed Internet access to homes—and to bring down the cost of high-bandwidth Internet access by essentially pooling access. Perhaps the grandest scheme belongs to SeattleWireless: rather than providing Internet connections, this group aims to build a free wireless infrastructure that allows any point in the city to talk to any other point—affording access to work files from home, for example.

These groups all have at least one thing in common. Their practice of "redistributing" bandwidth runs up against some legal obstacles. Most service agreements for DSL or cable

modem access essentially say, "'Thou shalt not carry other people's traffic,'" says Lenny Foner, founder of Somerville, MA-based wireless cooperative Davis-Net. Broadband Internet service providers are not keen on people sharing bandwidth. Indeed, AT&T Broadband spokesperson Sarah Duisik likens the practice to stealing cable TV. Regardless of its legality or morality, though, bandwidth sharing turns out to be tough for Internet service providers to detect. "For Davis-Net, we expect use will be barely above background," says Foner. Since most network users will only, say, check their e-mail or surf the Web, "the traffic isn't going to go up much. It's kind of tiny compared to the traffic one machine downloading MP3s generates."

The practice of redistributing bandwidth runs up against some legal obstacles, but it's also tough to detect. The technical hurdles might prove more difficult to clear.

NYCwireless hopes to avoid this problem altogether; it recommends that members who want to provide a gateway to the Internet carefully check their service agreements or make a contribution to help purchase a wholesale connection (the kind service providers themselves resell). The group has also established an "acceptable use" policy that all users must abide by, in part to shield the people who open their Internet access to wireless users from liability for any illegal activities in which those users might engage.

The legal issues can seem like a cakewalk next to the technical problems the networks face. The networks use an unlicensed part of the radio spectrum that, while free, is also crowded: cordless phones, ham radios and microwave ovens all operate at the same frequency. In addition, Federal Communications Commission regulations give priority to ham operators, satellite communications and industrial, scientific and medical users. If a wireless network interferes with any of those, it has to shut down. What's more, buildings, hills and trees can block the signals, which under ideal conditions travel perhaps 800 meters—only about 10 city blocks. As a result, it is difficult to create extensive networks in crowded cities.

Other issues that Wi-Fi networks face include the absence of built-in privacy mechanisms, the potential for unscrupulous users to hog bandwidth and what is known as the "roaming problem." (In a basic network setup, users who wander around will lose their connections as they move from one connection point to another.) While various groups are working on technical solutions to each of these problems, no one organization is trying to solve them all.

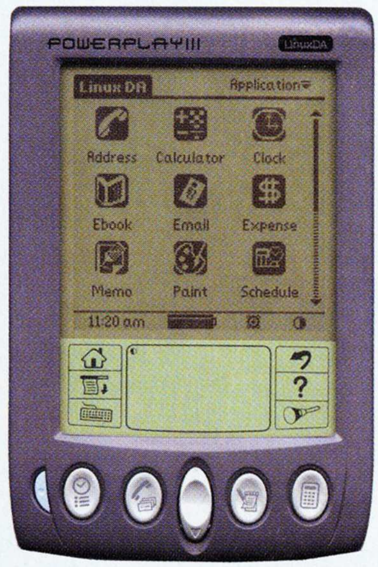
Despite the legal, regulatory and technical hurdles, cooperatively owned wireless networks are gaining popularity. Some see that trend as pointing to a revolution in the way people access the Internet. Mark Schultz, a senior associate at law firm Baker and McKenzie who works pro bono for NYCwireless, says, "You have to wonder whether it's going to be part of the infrastructure of the future, just like the streets or the electricity or the sewers and everything else. Whether Internet access is something we're all just going to have ubiquitous access to. That would be cool. And this may be a first step to that." —*Erika Jonietz*

LINUX IN YOUR PALM

SOFTWARE | Linux, the open-source operating system that some say could give Microsoft Windows a run for its money, is now taking aim at a new market: personal digital assistants. If the nonproprietary software can stake its claim in that area, it could help lay the foundations for a generation of less expensive handheld devices.

In recent months, there has been a surge of interest in Linux handhelds. Irvine, CA's Agenda Computing and Redmond, WA's Empower Technologies have started selling personal digital assistants that come preloaded with Linux, and several other companies now offer versions of Linux that can be installed on handheld devices—like the Compaq iPAQ—that normally run Microsoft's Pocket PC operating system.

Empower Technologies' Linux DA not only runs on Empower's own device but is the first distribution of a Linux-based operating system capable of running on the Palm handhelds, which have dominated the market for several years. Its designers overcame "a lot of technical barriers," according to Paul Leung, CEO of Empower, as Palms have only a fraction of the memory and processing power of the iPAQ and other handhelds.



Leung admits that few users will abandon the popular Palm operating system and its thousands of applications for Linux DA. Instead, he sees Linux DA as the beginning of a common operating system for a wide range of personal digital assistants. "We're trying to create a common platform that more manufacturers can support, giving people more choice," he says. Flooding the market with such clonelike devices could drive down prices, Leung says.

Industry analysts, however, are ambivalent about the prospects for Linux handhelds. Stacey Quandt of Cambridge, MA-based Giga Information Group says the idea is a viable one but adds that few people will buy a handheld simply because it runs Linux. "They will buy a device because of the applications it supports and if it provides enhanced functionality," she says. If the availability of compatible software remains limited, Quandt says, Linux handhelds "will be a hard sell." *—Jeff Foust*

COURTESY OF EMPOWER TECHNOLOGIES

NEW HUBS FOR NANO

NANOTECH | **Nanotechnology got a big boost last year when the federal government launched its National Nanotechnology Initiative, which will provide almost $520 million in funding in fiscal year 2002. As part of that initiative, the National Science Foundation is now funding six new applications-oriented nanotech centers.**

"These centers will give the field of nanotechnology high visibility," says Richard W. Siegel, who will direct one of the centers, located at Rensselaer Polytechnic Institute. "They will become magnets for people entering the field." Many of the new research units will be housed at already existing nanotech centers. But while those nanotech institutions are oriented toward understanding the fundamental scientific principles governing the field, each of the new centers will focus on specific applications of nanotech in areas such as electronics and medicine *(see table)*. Industrial partners like IBM and DuPont will help bring new technology to market.

The new center at Northwestern University, for instance, hopes to churn out highly sophisticated sensors by exploiting a technique for "writing" dense patterns of biological molecules on solid surfaces *(see "Nanotech Goes to Work,"* TR *January/February 2001)*. According to Chad Mirkin, director of the university's Institute of Nanotechnology, the patterned surfaces could lead to new kinds of detection systems for discovering drugs or diagnosing diseases. By supporting highly targeted efforts like these, the new centers hope to bring researchers one step closer to transforming nanoscience into real technology.
—Alexandra Stikeman

SIX CENTERS FUNDED BY THE NATIONAL SCIENCE FOUNDATION

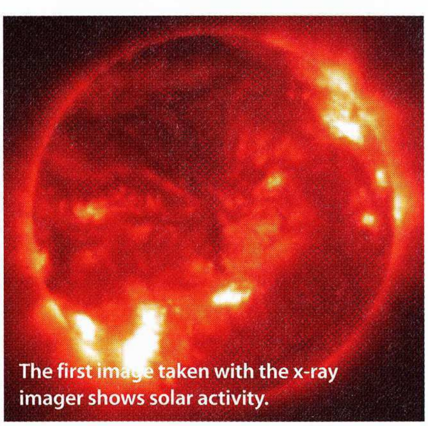
CENTER	LOCATION	FOCUS	FUNDING
Center for Integrated Nanopatterning and Detection Technologies	Northwestern University	Chemical and biological sensors	$11.1M/5 years
Center for Nanoscale Systems in Information Technology	Cornell University	Electronics, information storage and communications	$11.6M/5 years
Center for the Science of Nanoscale Systems and Their Device Applications	Harvard University	Electronic and magnetic devices and quantum information processing	$10.8M/5 years
Center for Electronic Transport in Molecular Nanostructures	Columbia University	Materials for electronics, photonics and biology	$10.8M/5 years
Center for Biological and Environmental Nanotechnology	Rice University	Materials for environmental engineering and medicine	$10.5M/5 years
Center for Directed Assembly of Nanostructures	Rensselaer Polytechnic Institute	Composites, drug delivery devices and sensors	$10.0M/5 years

HERE COMES THE SUN

SPACE | You might be worried about blizzards this winter, but what about coronal mass ejections? These giant blasts of electrified particles from the sun, along with solar winds and other space weather, frequently cause disturbances on earth, disrupting radio communications and inducing surges in power lines. But space weather forecasters could soon predict such events with better precision, thanks to a new imaging tool in use by the National Oceanic and Atmospheric Administration.

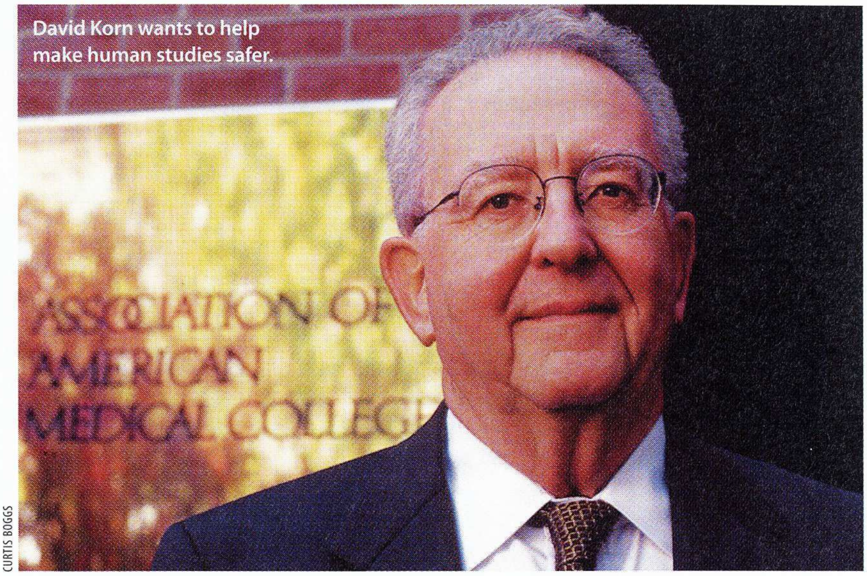
Strapped to a weather satellite, the new technology can detect solar flares, geomagnetic storms and other space weather events with far greater accuracy than present ground-based systems. The instrument consists of a telescope that captures x-rays emanating from the sun and a detector that converts the x-rays to visible light so images can be beamed to ground stations for analysis. Forecasters then get out the word via e-mail, fax and phone that, for example, a cloud of electrically charged gas is on its way to earth—a journey that can take anywhere from minutes to 36 hours. The alert can detail both where and when the space weather will arrive.

"We'll certainly see some things we haven't seen before," says Chris Balch of the Space Environment Center in Boulder, CO. That could help forecasters warn electric companies, say, that a surge was about to hit their power lines, in time for them to decrease output so the lines wouldn't be overloaded. NASA might even decide to change spacecraft orbits when a blast of radiation is predicted—helping astronauts stay safe from space storms. —*Kevin Hogan*



The first image taken with the x-ray imager shows solar activity.

COURTESY OF THE SPACE ENVIRONMENT CENTER



David Korn wants to help make human studies safer.

CURTIS BOGGS

SCRUTINIZING HUMAN RESEARCH

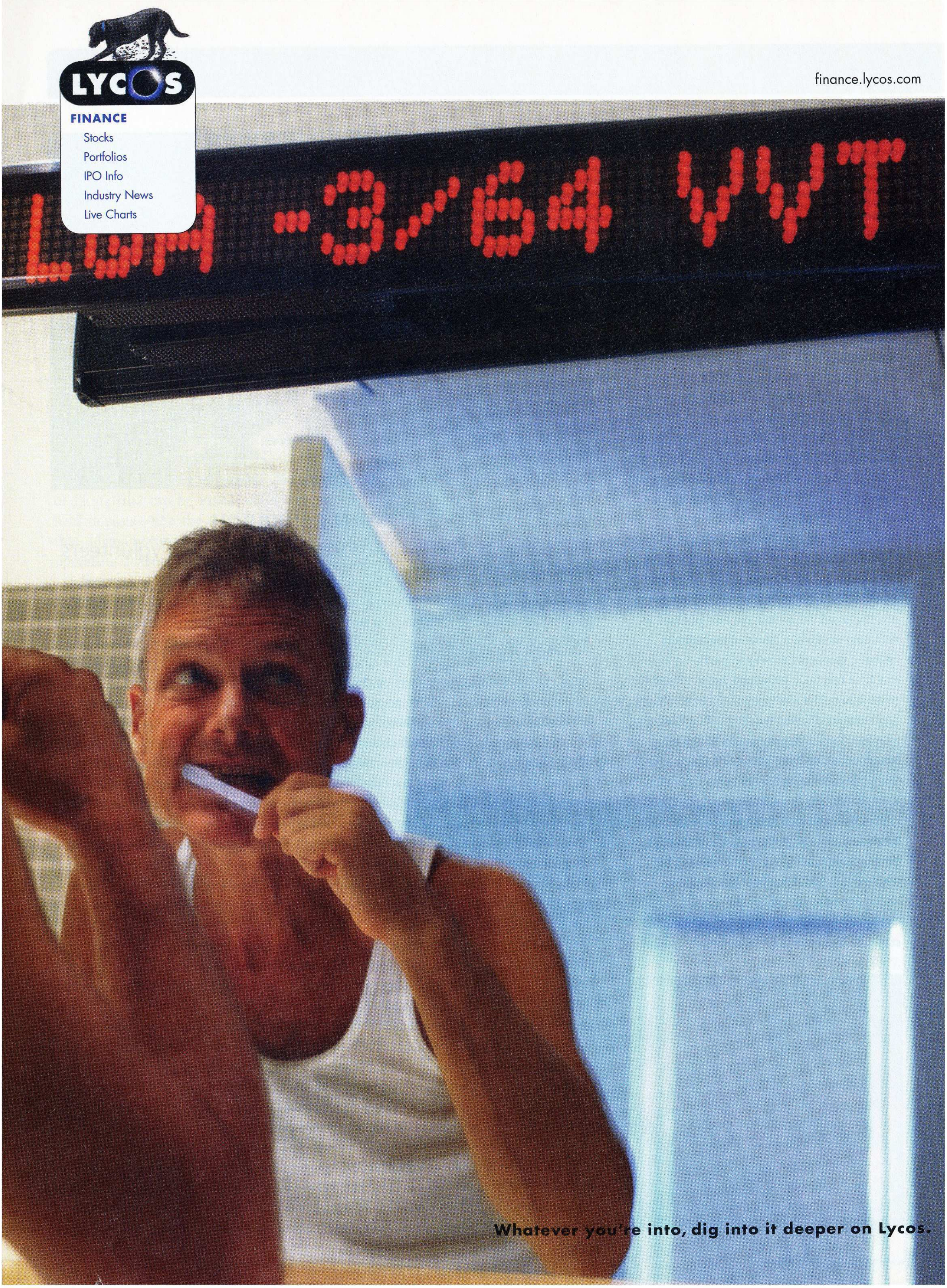
A new organization aims to protect research volunteers

MEDICINE | New medical treatments can be lifesaving—if they work. But for a volunteer in the experiments necessary to evaluate those hoped-for cures, the new treatments can be risky, even deadly. In the last few years, in fact, a number of research institutions have come under fire for not adequately protecting the health and rights of volunteers. Part of the problem, critics say, is that the federally mandated review boards whose responsibility it is to oversee human research at their respective institutions are often overburdened and lacking in the necessary expertise.

"Things get overlooked, short cuts are taken," says David Korn, a senior vice president of the nonprofit Association of American Medical Colleges. So this year Korn's group joined with six other nonprofit medical and research outfits to set standards for all U.S. institutions conducting human research and to promote those standards through a voluntary accreditation process. In contrast to federal inspectors, who tend to focus on record keeping, this new group will check that review boards have the experts to scrutinize complex studies, that the consent process for volunteers is ethical and that each study's risks are fully explained to volunteers.

Not everyone sees accreditation as the best route to cleaning up the mess. "It should be up to the government to enforce the rules and give more money to federal inspection agencies," says Leonard Glantz, associate dean of Boston University's School of Public Health. When the government shuts down a lab, Glantz says, the effect is much greater than when an institution loses its accreditation. Indeed, since 1998, the federal government has shut down, suspended or restricted research at over a dozen institutions. But officials at the U.S. Department of Health and Human Services say accreditation would send an important message about an institution's practices. And they welcome the help. "There's no way we can be all places at all times," says Bonnie Lee, a health issues analyst with the U.S. Food and Drug Administration. Accreditation may allow the FDA to concentrate less on random inspections of institutions, Lee says, and more on site visits in response to reports of misconduct.

Representatives of the biotech and pharmaceutical industries have also embraced the idea of accreditation, recognizing that their very survival depends on a public that perceives human research to be ethical and safe and is therefore willing to participate in it. The thousands of people who volunteer each year in the name of science are likely to welcome the new measure of safety too. —*Alexandra Stikeman*


LYCOS
FINANCE
Stocks
Portfolios
IPO Info
Industry News
Live Charts
finance.lycos.com
-3/64 VVT
Whatever you're into, dig into it deeper on Lycos.

COPYCAT CURES

Protein power, without the problems

BIOTECH | Proteins are key players in the biological processes that determine whether a person is sick or well. So not surprisingly, they form the basis for some of today's most important and effective drugs. But in some ways, these large, complex biomolecules are far from being the perfect drugs: they're chewed up in the stomach if taken by mouth, and many of them break down even when injected—severely limiting which proteins can be used. Now a number of biotech companies are reporting progress in designing smaller, more stable molecules that mimic the therapeutic action of proteins, opening the door to completely new drugs, and to the possibility of replacing some painful injections with equally effective pills.

In July, MetaPhore Pharmaceuticals of St. Louis announced the successful safety testing in humans of a "mimetic"—a drug that mimics the action of a human protein. The new drug is a copycat of a natural enzyme that disarms toxic free radicals, and it could eventually be used to treat cancer, arthritis, pain and even the aging process. But beyond all that, the drug demonstrates that a small engineered molecule can, in fact, take the place of a pharmaceutical protein.

Mimicking a protein was an accomplishment considered impossible just a decade ago, says Adrian Whitty, a senior scientist at Cambridge, MA, biotech giant Biogen. Only proteins, he explains, were thought capable of carrying out complex functions like, for example, triggering a chain of events inside a cell by binding to certain receptors on its surface. But in the mid-1990s, several groups showed that smaller molecules, initially found by random screening, could actually do the same job by binding to "hot spots" on those receptors. Since then, researchers have used either screening or computers to find or design more such targeted molecules, giving birth to mimetics.

A handful of companies have formed to tap mimetics' potential *(see table)*. Locus Discovery, a Philadelphia-area startup, and Palo Alto, CA's Affymax each say they have developed mimetics of erythropoietin, biotech's best-selling protein-based drug, which helps reverse anemia caused by chemotherapy and kidney dialysis. Since erythropoietin must now be injected, a mimetic-based pill would be poised to capture its $6 billion market. If such pills can prove themselves in clinical trials, it could mark the end of painful injections for many patients. —*Ken Garber*

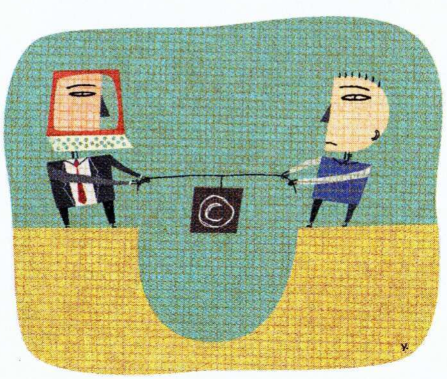
FIRMS IN MIMETICS

COMPANY	DISEASE TARGETS
MetaPhore Pharmaceuticals (St. Louis, MO)	Cancer, pain, stroke
Eukarion (Bedford, MA)	Radiation damage in cancer, neurodegenerative disease
Incara Pharmaceuticals (Research Triangle Park, NC)	Radiation damage in cancer
Locus Discovery (Blue Bell, PA)	Cancer, kidney failure
Affymax (Palo Alto, CA)	Cancer, kidney failure
Praecis Pharmaceuticals (Waltham, MA)	AIDS, prostate cancer

COPYRIGHT CONTROL

INTERNET | **Publishers of newspapers, magazines and other written media all face a common dilemma: how can they distribute—and profit from—copyrighted material online without opening their content to piracy? A new system from an old player in the copyright management arena, Danvers, MA-based Copyright Clearance Center, might offer an answer.**

The Copyright Clearance Center manages conventional copyrights for thousands of publishers (including *Technology Review*). Its new online system uses a plug-in—software that works in concert with a Web browser—to let users view, copy, save and print specific content, or to prevent any of those actions, based on fees paid online or over the phone. Without such software, most publishers have had few options: granting readers free, unlimited online access to their content; granting access based on a subscription system where users pay whether or not they use materials; or charging one-time fees for archived articles. But unlike the Copyright Clearance Center's technology, none of these schemes can prevent a user from illegally copying or distributing the content once he or she has paid any relevant fees.



JAMES YANG

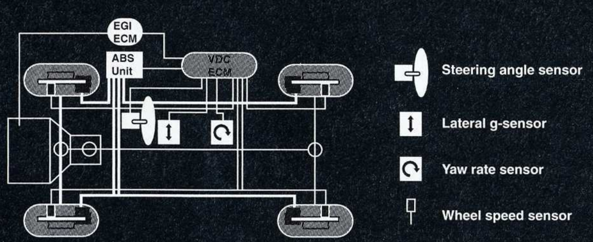
Other companies, like Renton, WA's iCopyright.com, are also introducing technological cures for online publishing woes. But decades of experience in the paper world could give the Copyright Clearance Center a leg up.

Still, while the company's system is an important first step, says Bill Rosenblatt, president of New York-based management consultancy GiantSteps/Media Technology Strategies, it might already be behind the curve. That's because the sort of documents the software manages, such as newspaper and magazine articles, are already moving from laptops and desktops to mobile devices such as handheld computers and cell phones, and these devices are currently beyond the reach of the Copyright Clearance Center's software. All of which could spell new trouble for beleaguered publishers. —*David J. Wallace*

ENGINEERED TO BE ALMOST PSYCHIC.

Introducing a car so technologically advanced, it can sense trouble and begin to adjust for it before the driver even notices there's a problem. It's the 6-cylinder 212-horsepower Subaru Outback VDC.

The VDC stands for Vehicle Dynamics Control, a highly intelligent stability system that's designed to help prevent loss of control due to conditions like oversteer, understeer, wheel spin or vehicle drift. Ingeniously coupled with full-time Subaru All-Wheel Drive, it rivals systems found in vehicles costing thousands more.



The heart of VDC is a sophisticated series of sensors that continually monitor steering angle, wheel speed, brake pressure, yaw rate and lateral g-forces. The instant a difference is detected between the driver's intended direction of travel and the path the car is actually taking, VDC takes corrective action. Momentary brake pressure may be applied to individual wheels. The All-Wheel Drive system may redistribute the amount of power between the wheels. Even the engine's output may be momentarily reduced. Before the driver even realizes that loss of control is impending, any or all of these measures may be automatically applied to help restore directional stability. It's almost as if the car has a sixth sense.

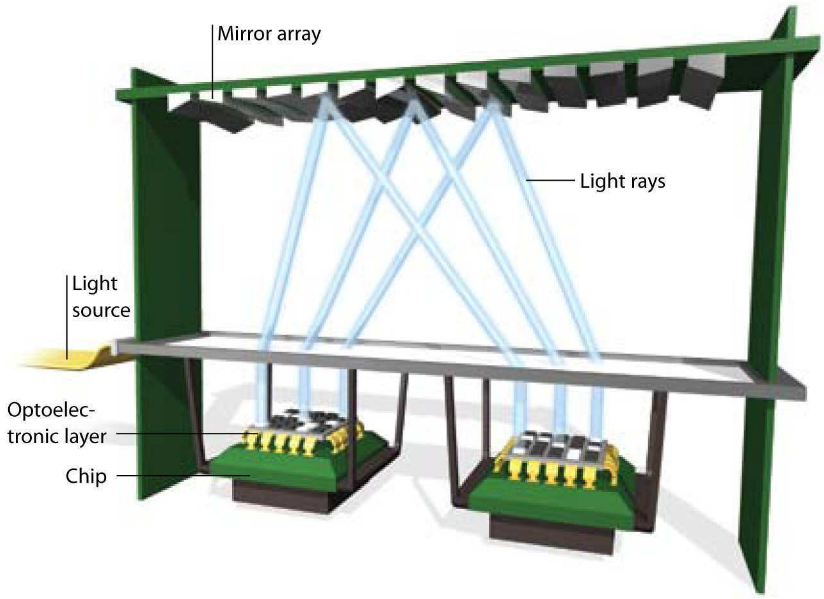
In fact, in every sense the Outback VDC is a remarkable vehicle. With tactile luxuries like a leather-trimmed, 8-way power driver's seat. A mahogany and leather steering wheel by Momo®. And a state-of-the-art 200-watt* sound system built exclusively for Subaru by McIntosh®. Working together, McIntosh and Subaru engineers placed 11 speakers in 7 strategic locations so the audio quality would be specifically tuned to the car's unique acoustics.

The Outback VDC from Subaru. It is truly a phenomenon in the world of automotive engineering. And we have a feeling you're going to love it. To find out more, come visit us at **www.subaru.com**.

OUTBACK® VDC

The ABC's of Safety: Air bags. Buckle up. Children in back.
*At maximum output


SUBARU
The Beauty of All-Wheel Drive.



SLIM FILMS; SOURCE: DAVID MILLER

In technology developed by David Miller, light signals are transmitted by optoelectronic material on a chip; the chip's electronics control the signal. Mirrors guide the light to a neighboring chip.

OPTICAL INTERCONNECTS

Transporting data at the speed of light

Networks of optical fibers speed massive amounts of data around the world, enabling the Internet and changing the very nature of communications. Now engineers and physicists are seeking ways to adapt optical systems to move data from point to point inside computers. If these so-called optical interconnects are successfully developed, they could allow computers to share more information among their components more quickly; without them, the continuous increases in computing speed and power that we now take for granted could abruptly level off.

Data in computers currently move across chips and from chip to chip electronically, through tiny metal wires. But as computers get faster and faster, manipulating ever more data, these wires are just not up to the task: it's a bit like connecting to the Internet over the phone instead of a broadband link. Moving data to a computer's central processor from its memory, for example, is already a notorious bottleneck; the wires simply can't ship data from memory fast enough to keep the processor busy. And the problem is only going to get worse.

Making the metal interconnects from copper instead of aluminum—technology pioneered by IBM—and tweaking designs will help. But within five years, experts say, they may not be able to push electronic signaling any further.

Systems that replace wires with optics will ultimately move data faster, use less power and transport data more accurately at high speeds. Computer designers are already taking the first steps to make such systems. Agilent Labs and University of Southern California electrical engineer Anthony F. J. Levi have jointly adapted fiber-optic technology to link high-performance computers like servers into networks. The technology, which Agilent commercialized last year, is used to connect the machines over distances of about two to 500 meters. The optics maximize the usage of available computing power by making data transfer within the network more than 50 times faster than is possible using copper cables.

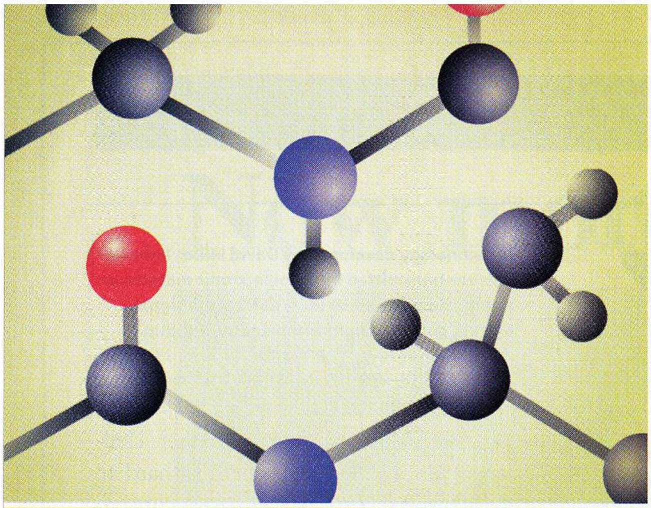
To push optical connections down to the chip level, engineers must develop ways to generate and receive light signals on semiconducting devices. The crucial breakthrough for Agilent's network links was adapting tiny semiconductor lightwave devices called vertical-cavity surface-emitting lasers. Waguih Ishak, director of Agilent's Communications and Optics Research Laboratory, believes these lasers can be adapted for use inside computers as well.

But engineers face a further challenge. Unlike electricity, light is hard to steer through very small spaces: conventional optical fibers wildly scatter light if subjected to tiny twists and turns. Therefore, to transmit the signals generated by the lasers, the researchers need new ways to direct light through the tight confines of a circuit board.

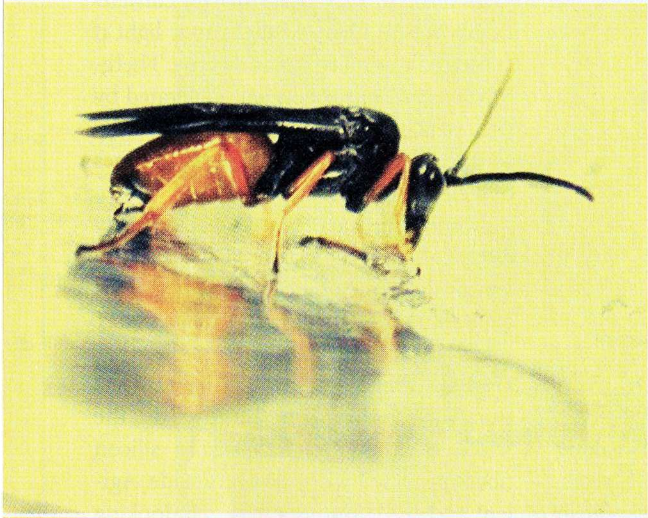
Strategies vary. Stanford University electrical engineer David Miller plans to simply guide the photons through tiny air gaps using mirrors *(see illustration)*. MIT materials scientist Lionel Kimerling has created waveguides only 200 nanometers thick—less than one-hundredth the width of a human hair—from silicon fibers insulated with silicon dioxide. Agilent and IBM, among others, are looking to make waveguides from materials called photonic crystals *(see "Microphotonics,"* TR *January/February 2001)*; the materials act as miniaturized optical fibers. With photonic crystals, "You can manipulate both the optical and electronics on the same scale," says Gian-Luca Bona, head of the Photonic Networks Group at IBM's Zurich Research Laboratory.

Within five to 10 years, researchers say, optical interconnects will begin appearing in high-end computers; eventually, optics will make their way into home computers. Such computers will be fast enough to handle the flood of information coming through the fiber-optic cables that will one day stretch into homes. And with chips ready to accept optical data, the link between computers and data pipes will be fairly simple.

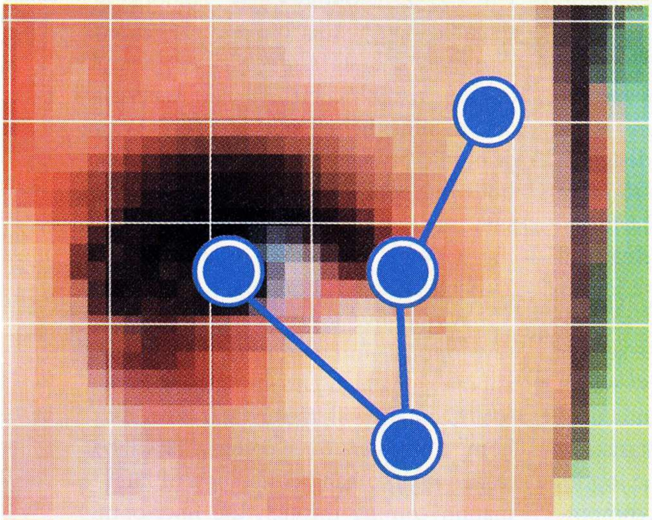
"There's not a breakthrough needed to do this," says Miller. "But we have a lot of research to do." Still, Levi is already planning for the day when this all-optical vision becomes reality: "When fiber-to-the-home happens, you will want fiber-to-the-processor-based systems in your home—to look at real-time holograms of the grandkids." *—Erika Jonietz*



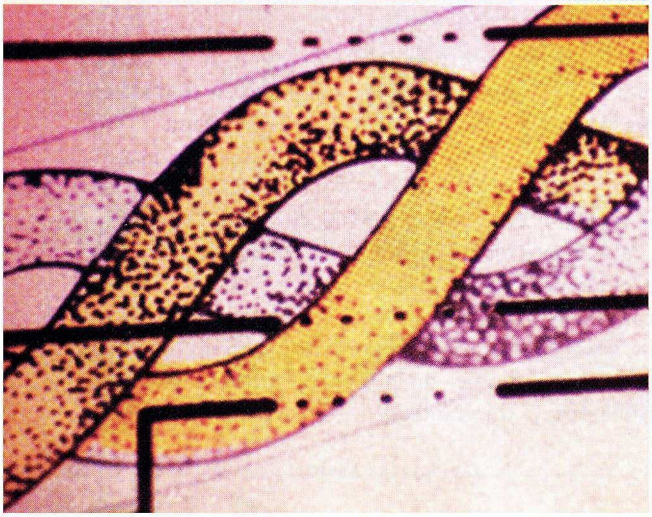
MATTHEW BOUCHARD



COURTESY OF GLEN RAINS



PHOTODISC



PHOTODISC

AN MIT ENTERPRISE

TECHNOLOGY REVIEW ONLINE

www.technologyreview.com

MORE INFOTECH
MORE BIOTECH
MORE NANOTECH

TWICE AS MANY STORIES
UPDATED DAILY

INFOTECH ▶

All the News That's Fit for You
Microsoft's prototype video clipping service aims to ease your information overload.

Visualize: Face Recognition
How do security systems spot a face in the crowd? **[Multimedia]**

BIOTECH ▶

Designer Genes Reconsidered
People with wings and gills may not be such a bad idea, claims a prominent bioethicist.

Power Tools for Proteomics
How researchers chart the largely unexplored world of proteins.

NANOTECH ▶

Nanobiotic Lifesavers
Peptide rings self-assemble into antibiotic nanotubes that puncture deadly bacteria.

Nanotech's Super Models
Simulation teams unravel the mysteries of the mesoscale.

EXTRA ▶

High-Speed Trains Are Catching Up
Taking a cue from Europe and Japan, the U.S. gets on track with high-speed trains.

Bugs Smell Success
Human technology may be taking a backseat to nature in the detection of crop disease.

PLUS:

- ▶ **FREE NEWSLETTER**
  Our weekly e-newsletter brings emerging technologies to you.
- ▶ **TECHNOLOGY REVIEW ARCHIVE**
  Pore through back issues online, whenever you want.
- ▶ **VISUALIZE IT ONLINE**
  Animations of our popular Visualize column explain key technologies.
- ▶ **OFF THE WIRE**
  Each day, we select the most interesting technology news stories.
- ▶ **TECHNOLOGY REVIEW ON THE AIR**
  View Editor in Chief John Benditt's monthly analysis of emerging technologies on CNBC.

DOCTORS WITHOUT PATENTS

The French government has frequently acted to protect its native commerce. France has subsidized its indigenous film industry to shield it against Hollywood competition; a French regulatory organization even went to court to insist that only French-grown sparkling wines bear the coveted name "champagne."

Now a respected French institution is campaigning to protect its medical research community. Only this time, the case has implications far beyond the nation's chauvinist interests. The Institut Curie, a top center for cancer research and treatment, announced recently that it will try to overturn a patent issued to a U.S. biotech firm conferring exclusive rights to breast cancer screening tests. Curie representatives contend they are combating "an unacceptable monopoly."

The contested patent, granted last January by the European Patent Office to Salt Lake City-based Myriad Genetics, covers diagnostic tests using the BRCA1 gene to screen for a genetic predisposition to breast cancer (about one-half of inherited breast cancers are associated with this gene). Myriad Genetics won a similar U.S. patent in 1998 and now holds a broad patent portfolio over the BRCA1 gene in much of the world. What makes the case noteworthy is the core French argument: that Myriad Genetics' monopoly on a diagnostic test runs counter to France's "conception of public health." It is a potent argument, and not just in France. The world's patent systems face perhaps their most vexing challenges when proprietary rights clash with doctors' age-old practice of freely sharing health-care know-how.

WEBB CHAPPELL

With support from the French Ministry of Health and Ministry of Research, the Institut Curie offers substantial evidence to bolster its claim. Dominique Stoppa-Lyonnet, head of oncological genetics, charges that Myriad's unwillingness to license its technology means that French doctors wishing to screen their patients for predisposition to breast cancer must now send all DNA samples to Myriad for analysis. Myriad's test costs some $2,500—more than three times the cost of existing French tests—and will preclude some 17 French laboratories from carrying out diagnostic research based on the results. Aside from the detriment to French patients, she says, "Giving in to this monopoly would bring about an intolerable loss of data and expertise for French laboratories."

The Institut Curie also contends Myriad's patent is too broad, covering existing as well as any future BRCA1-based screening techniques. European patent attorney Jacques Warcoin says the patent will thus stifle innovation in France. He also notes that identification of the BRCA1 gene was made possible by the work of many research teams, as well as with the collaboration of women from at-risk families. What's more, that groundwork helped geneticist Mary-Claire King of the University of California, Berkeley, accomplish the key step of assessing 183 possible genetic markers for breast cancer and narrowing the list to one on chromosome 17. King published her team's work in late 1990; on the strength of her findings, Myriad isolated the BRCA1 gene some four years later.

William Hockett, a Myriad spokesperson, dismisses such claims, saying, "Patents allow new technology to develop—in this case, very high quality tests." Hockett notes that his firm doesn't license its patent in order to offer "the highest-quality tests possible." Quality control is paramount, he says, because screening tests influence critical decisions on patient care. Hockett also says it is "absurd" to charge that Myriad wants to stifle breast cancer research. He stresses that his firm is a major sponsor of such research, in part because—given the strength of its patent portfolio—"it benefits us directly."

But Myriad's statements do little to alter the real issue: namely, the clash between public health and proprietary claims on medical know-how. Traditionally, most patent systems distinguished between medical devices—like pacemakers—which can be patented, and medical procedures, such as the Heimlich maneuver, which have usually been freely shared by medical practitioners. Diagnostic tests, and even many drugs and vaccines, have fallen into an uncomfortable gray area: on the one hand they require some manufacturing (a feature often linked with patentability), while on the other hand they result increasingly from advances in the conceptual medical know-how that has been shared among doctors for at least the 2,000-odd years the Hippocratic oath has existed.

A French challenge to a gene-based-breast-cancer-screening patent shows how proprietary rights increasingly clash with doctors' age-old tradition of freely sharing health-care know-how.

With the exception of the United States, some 80 countries, including every European Union nation, already exempt medical procedures from intellectual-property protection in order to safeguard the dissemination of new medical techniques and knowledge. As Europe grapples with diagnostic tests based on gene patenting, the gray area of useful medical knowledge grows. The Curie Institute's legal action is an important protest. But more proactive work is needed to clarify appropriate limits on similar health-care claims. Ideally, a panel of stakeholders under the auspices of an international body like the World Health Organization ought to tackle the job. Without such a group, we will likely see many divisive fights like this one—needlessly restricting medical knowledge and potentially undermining the Hippocratic oath. TR

To join an online discussion of this article, visit www.technologyreview.com/forums/shulman

Virus detection: Dr. Kenneth Mandl of Children's Hospital Boston says "bio-surveillance" tools would mine data for early signs of epidemics.

By David Talbot Photograph by Beth Perkins

Detecting Bioterrorism

Moving up the technology agenda: sensors that sniff out bio-agents and software that fingers epidemics.

As always for a presidential inaugural, security and surveillance were extremely tight in Washington, DC, last January. But as George W. Bush prepared to take the oath of office, security planners installed an extra layer of protection: a prototype software system to detect a biological attack. The U.S. Department of Defense, together with regional health and emergency-planning agencies, distributed a special patient-query sheet to military clinics, civilian hospitals and even aid stations along the parade route and at the inaugural balls. Software quickly analyzed complaints of seven key symptoms—from rashes to sore throats—for patterns that might indicate the early stages of a bio-attack. There was a brief scare: the system noticed a surge in flulike symptoms at military clinics. Thankfully, tests confirmed it was just that—the flu.

While the January monitoring revealed nothing unusual, the deployment was just one more indicator that, long before the September 11 attacks and subsequent letter-borne anthrax assaults, U.S. security experts were taking seriously the threat of a large-scale biological attack. And for good reason. Not only could bio-agents covertly released by terrorists potentially kill hundreds of thousands, but they are extremely difficult—with currently available technology—to detect in the environment. A successful attack with biological agents—anthrax, smallpox and bubonic plague top the most-feared list—might only become clear days later, when people became seriously ill and were beyond the help of available treatments. And unlike anthrax, many bio-agents are contagious, so in any time lapse before health officials recognized an attack, victims could multiply its effect by spreading disease to others.

Already, terrorists have shown they can obtain and deliver anthrax on a small scale, and experts believe a determined group could conceivably accomplish a much larger-scale bio-attack—though it wouldn't be easy. "The level of sophistication that went into the World Trade Center attack, if applied to a chemical or biological attack, could produce an effective effort," says George Whitesides, a Harvard University chemist researching treatments for anthrax. "It is technically feasible. Whether it is politically or operationally feasible, and at what scale, we don't know. Nonetheless, we will have to prepare for the possibility, because we need an insurance policy."

That insurance policy will likely include a broad array of new technologies on at least three fronts: improved portable devices to detect and identify biological agents; new data-mining efforts to seek subtle bio-attack indicators like a spike in certain patient symptoms at emergency rooms; and improved therapies for victims. A number of these technologies have been under development for years, but in the aftermath of September 11, they're getting a renewed burst of attention from government, academic and industrial researchers.

The urgency is felt because current technologies are not ideal for meeting the threat; for one thing, they can't provide continuous air monitoring. Existing portable, briefcase-sized devices—including one from Sunnyvale, CA-based Cepheid that adapts established laboratory DNA tests—can identify pathogens in 15 to 20 minutes, and state and federal public-health laboratories are now widely using them for rapid, precise identification of suspected anthrax strains and other pathogens. But the devices only work with liquid samples—like water from a reservoir, or a sample swabbed from a solid surface—that generally take an hour or more to prepare. According to most experts, however, an airborne attack is more likely than a water-borne one and could be far more damaging.

In the coming months, the U.S. Department of Defense hopes to roll out a new truck- or ship-mounted system

that continually samples and tests air for worrisome pathogens, says Calvin Chue, a microbiologist at the Center for Civilian Biodefense Studies at Johns Hopkins's Bloomberg School of Public Health. The system, being manufactured by DeLand, FL-based Intellitec and Columbus, OH-based Battelle, uses a laser system and software developed at MIT's Lincoln Laboratory to continually screen microscopic particles in the air. When something worrisome shows up, a detector mixes an air sample into a solution and tests for up to 10 pathogens using thin paper strips, each bearing antibodies for an anticipated biological agent *(see "Sensing Airborne Pathogens," opposite)*. The device can operate autonomously, beaming results back to a base station; new cartridges can be inserted to test for different pathogens. In addition, Cepheid is adapting its detection system for use in the air sampler.

But existing antibody- and DNA-based detectors are limited in the number of pathogens they can identify. Future portable sensors are expected to use DNA chips that could screen for hundreds of possible threats. These chips carry small fragments of DNA from pathogens that could serve as bioweapons; the fragments bind to any complementary pathogen DNA that might be present. Using such chips to detect bio-agents is now possible but requires a lab full of equipment to prepare samples and analyze the results. "If we could shrink those down in a portable, fieldable unit," Chue says, "you could look at hundreds of organisms, potentially in 10 to 15 minutes." In the late 1990s, Affymetrix, a leading DNA chip maker, built a prototype system about the size of a large microwave oven. "There's a fair bit of work needed" to turn it into a practical field device, says Robert Lipshutz, Affymetrix's vice president for corporate development. "We're not saying where that program is at this time." Like the existing sensors, Affymetrix's detector will only work on liquid samples, but Bill Altman, biosensor program manager for Battelle, says DNA chip systems could be adapted to work together with an air sampler, creating a powerful, versatile bioterrorism monitor.

Farther on the horizon are sensors that would harness the exquisite sensitivity of live cells to detect biological agents. While DNA arrays can only detect what they've been set up to find, whole-cell sensors could reveal unforeseen agents. These systems can also determine whether a pathogen is alive or dead—key to establishing its virulence—and eliminate the need to preprocess samples. Dozens of academic, corporate and federal labs are working on the technology. And while each version functions differently depending on the kind of cell being used—heart cells, neurons, white blood cells and liver cells are among those being tested—they operate on the same basic principles. When a pathogen invades a cell, the cell releases proteins, changes size or alters its metabolic rate; sensors can measure these changes electrically or optically.

"A LARGE-SCALE BIO-ATTACK IS TECHNICALLY FEASIBLE. WE NEED AN INSURANCE POLICY"—INCLUDING DEPLOYMENT OF NEW TECHNOLOGIES.

But using cells as sensors is tricky; a detection device would require systems to keep cells alive and nourished. Although whole-cell sensors are probably two to five years away from field use, a clear sense of urgency has gripped the research community. "There is a palpable feeling that we need to bust ass and get this thing out," says MIT chemical engineer Linda Griffith, who is developing a liver-cell-based sensor chip to detect bio-agents like aflatoxin, a compound produced by fungi, which attacks the liver.

With airborne-pathogen detectors still in the lab, just realizing that an attack is under way could take precious time. So computer scientists are developing warning systems to spot early indicators of a biological attack, from troubling trends in patient symptoms to increases in school absenteeism. Known as bio-surveillance, the field aims to use data-mining techniques to recognize an epidemic days before the first cases are confirmed, says Kenneth Mandl, a pediatric emergency physician and informatics researcher at Children's Hospital Boston.

Mandl and colleagues at MIT's Laboratory for Computer Science have devised a computerized tracking system that uses emergency-room intake information to monitor the frequency of rashes, fevers, coughs and intestinal problems, symptoms associated with common ailments that would appear in uncommonly large numbers in the event of a deadly biological attack. Effectively protecting a city or large population, however, requires linking reports from many medical facilities. Mandl and his counterparts at other hospitals are now working on a system that would do just that. It's more difficult than it sounds; hospitals use a hodgepodge of computer programs and don't collect patient information in uniform ways. Still, Mandl says, "it's an important public-health measure to take. Most likely, the way this will eventually happen on a large scale is when it becomes a mandated reporting obligation."

It was just this type of system that the U.S. military tested at Bush's inaugural. Its detection of a flu outbreak was an encouraging sign that such a system could sniff out—and make sense of—a particular pattern of symptoms. Now, efforts sponsored by the Department of Defense are under way to build a far more sophisticated early-warning system that would look beyond hospital information to include more subtle trends like hits on health-related Web sites, purchases at pharmacies and grocery stores (think orange juice and cough syrup), school attendance—even visits and inquiries at veterinary clinics and agriculture offices, since a bio-attack could affect animals and plants, too. Researchers at university, corporate and military labs are working on elements of this ultimate bio-surveillance tool; a prototype is due in 2004.

Even with early warning from bio-surveillance software and sensors, victims of a biological attack could face grim survival odds; 30 percent of smallpox sufferers die, as does nearly everyone who inhales or ingests anthrax and

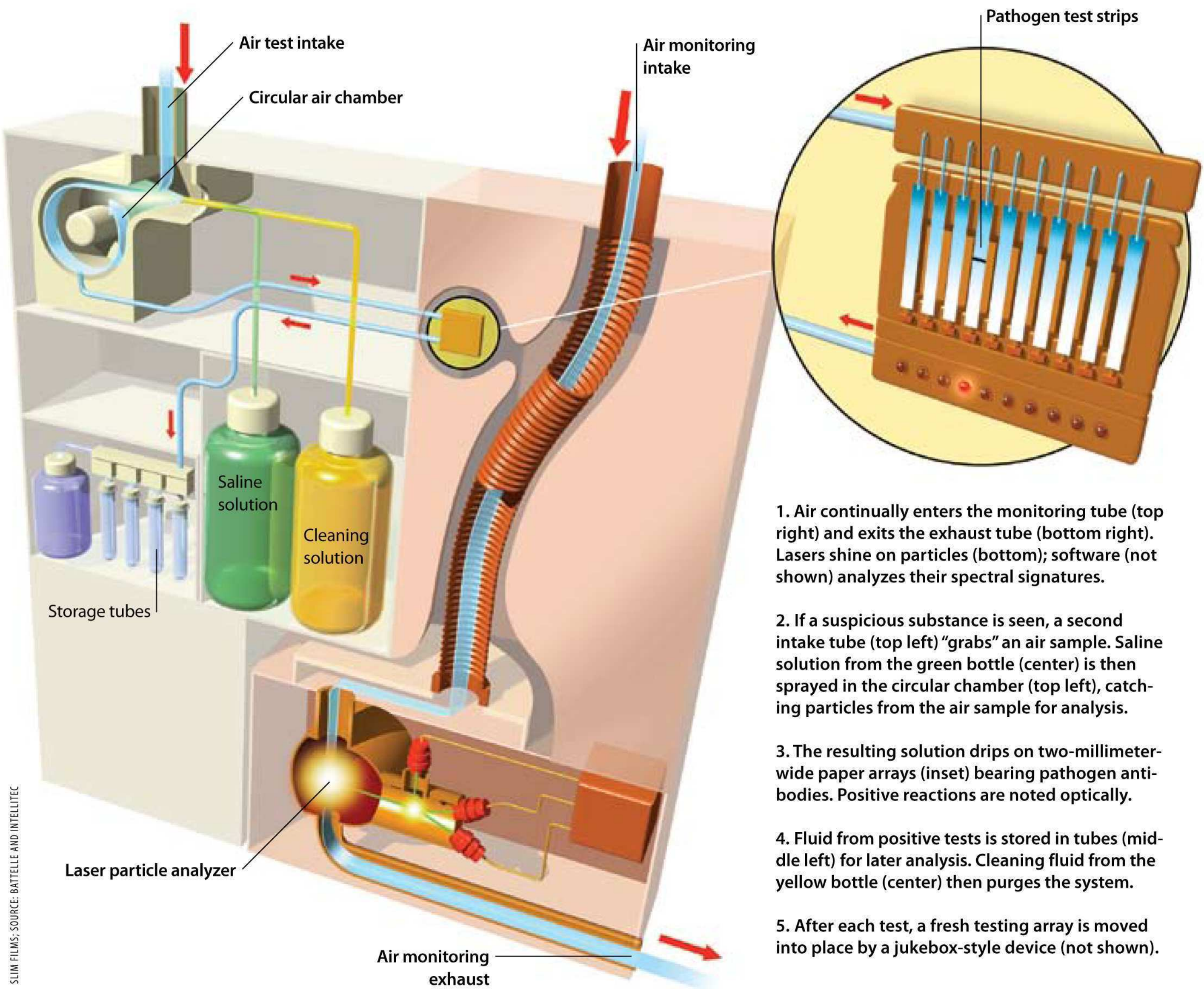
doesn't quickly get antibiotics. To improve those odds, health officials are stockpiling vaccines; with smallpox inoculations discontinued in the 1970s, for example, and the vaccine effective for only about 10 years, the U.S. population is susceptible to infection. Last year, the U.S. Centers for Disease Control and Prevention contracted Cambridge, MA-based Acambis to provide 40 million doses of smallpox vaccine over 20 years. The vaccine could both protect the unaffected and save the lives of those already infected by decreasing the severity of the disease. And one month after the terror attacks, the Bush administration greatly accelerated this effort, asking Congress for $509 million to buy 300 million doses to be delivered in 2002.

Researchers are also developing treatments to combat other diseases caused by bio-agents. An anthrax antidote developed by Harvard's Whitesides and Harvard Medical School microbiologist R. John Collier is in the pipeline. In early tests, the treatment has cured rats exposed to anthrax toxin. The anthrax bacterium produces both a deadly toxin and a protein that creates a donut-shaped channel in the wall of a target cell to let the toxin in. The potential drug consists of a molecule that acts like a strip of Velcro, binding to the donut and shutting out the toxin. Collier says he plans to further study this treatment using actual anthrax stored at military facilities. "There is a lot of activity right now in putting together a biotech company that will work closely with government agencies to develop this rapidly," he says.

No level of preparedness—and no technological advances—can completely eliminate the threat of biowarfare. But as researchers at labs around the country begin delivering technology that sniffs the air and watches hospitals, that threat should become a whole lot smaller. TR

Sensing Airborne Pathogens

A U.S. Department of Defense bio-agent detector to monitor and test the air for pathogens is near deployment.



1. Air continually enters the monitoring tube (top right) and exits the exhaust tube (bottom right). Lasers shine on particles (bottom); software (not shown) analyzes their spectral signatures.

2. If a suspicious substance is seen, a second intake tube (top left) "grabs" an air sample. Saline solution from the green bottle (center) is then sprayed in the circular chamber (top left), catching particles from the air sample for analysis.

3. The resulting solution drips on two-millimeter-wide paper arrays (inset) bearing pathogen antibodies. Positive reactions are noted optically.

4. Fluid from positive tests is stored in tubes (middle left) for later analysis. Cleaning fluid from the yellow bottle (center) then purges the system.

5. After each test, a fresh testing array is moved into place by a jukebox-style device (not shown).

SLIM FILMS; SOURCE: BATTELLE AND INTELLITEC

Missing links: MIT's Franz-Josef Ulm is testing the idea of an "intelligent city"—a centrally monitored metropolis linked in real time over the Web.

By Wade Roush   Photograph by Robert Delahanty

Networking the Infrastructure

The technology of redundancy could lead to smarter cities, designed to alert us of danger.

It's a gray late-September Sunday in San Francisco, a few weeks after the carnage at the World Trade Center, and my dog and I are walking along the beach near the Golden Gate Bridge. The huge structure seems graceful, spare and absolutely immovable. Yet with a brain steeped in movie special effects and, now, the all-too-real TV images of September 11, I can't help imagining the scene if a 767 were to rocket down out of the clouds, decapitating one of the bridge's towers or snapping the main suspension cables. I can see wires recoiling in slow motion, the main span sagging and shearing apart, cars and trucks and pedestrians plunging into the bay 67 meters below.

How many people are imagining similar horrors in their own cities, where the skylines remain unscathed? Ever since the seemingly invincible Twin Towers disappeared in a cloud of dust, Americans have been spooked about the danger to the national infrastructure. Naturally, we're wondering if anything can be done to harden skyscrapers against suicide attacks. But we're also reexamining our entire technological fabric—buildings and bridges and tunnels, stadiums and train stations and shopping malls, water supplies and the electrical grid, computer and telephone networks, roads and railways—and asking how it can be made more resistant to the predations of terrorists. "We have to start envisioning, and preparing for, worst-case scenarios," says Nancy Greene, president of the American Civil Defense Association, a Starke, FL-based nonprofit organization dedicated to preparing the population for natural and unnatural disasters. "People are finally starting to wake up, but unfortunately it takes this sort of action to make it happen."

The good news, say Greene and other experts paid to think about such things, is that there is little call for catastrophism. The country's sheer size and the distributed nature of many aspects of the infrastructure—from roads to centers of commerce to communications—limit the amount of disruption any single terrorist group could cause. But that kind of resilience is weak in other interconnected systems such as the power grid and our water system and even missing entirely from the structural framework of buildings and cities. If engineers could beef up those interconnections already in existence and introduce them where they're nonexistent, we could limit the damage from an attack even further.

The key lies in developing and deploying technologies that will tie infrastructure components together into a system that's far smarter and more self-aware than anything we have today. Engineers, security consultants and authorities on counterterrorism are working hard to weave together the threads of this technological fabric, which will be pervaded by instruments that can sense harmful chemicals in a reservoir, relay critical data about a damaged building's structural integrity to rescue workers, help map escape routes or streamline the flow of electricity in a crisis. These high-tech networks—joined with simulation tools, enhanced communications channels and safer building designs—could go a long way toward creating an "intelligent city," where danger can be pinpointed and emergency response directed with precision.

THE POWER OF DIVERSITY

The template for this new, more secure infrastructure—already replete with interconnected redundancy and a kind of intelligence—is the Internet. Its underlying packet-switching protocol allows data blocks such as e-mail messages to be chopped up, scattered through the network via whatever pathways are open, and reassembled by the addressee. The destruction of one or even several routes may slow down data but doesn't prevent it from reaching its final destination. "The Internet was designed to survive nuclear war, so it will automatically route around disruptions. That's a good model for thinking about some of the other things like electricity and the 911 system," says James Andrew Lewis, a senior fellow and director of technology policy at the Center for Strategic and International Studies in Washington, DC.

The nation's water supplies already share some of the Internet's hardiness. Rare is the city that depends on a single source for its water. New York City, for instance, draws water from 19 reservoirs and three lakes in upstate New York via an interconnected network of tunnels and aqueducts. If terrorists were to blow up one aqueduct, the others would still flow. If they were to dump biological agents such as botulinum toxin into one reservoir, it could theoretically be cut off from the system until purified.

But much more could be done to keep drinking water safe. For example, "We could instrument our reservoirs [to detect contaminants] very cost effectively and very quickly," suggests Roger McCarthy, chairman of Menlo Park, CA-based Exponent Failure Analysis Associates, which consults with industry and government on disaster response and readiness. In fact, the U.S. Environmental Protection Agency was granted $2.5 million in federal funding this year for research on bioterrorism, including the development of new technology for detecting biological agents in water *(see "Detecting Bioterrorism," p. 34)*. And researchers at Sandia National Laboratories in Albuquerque, NM, are already field-testing tiny electronic sensors that can be lowered into reservoirs or underground wells to sniff for toxic chemicals. The sensors contain "chemiresistor" chips that measure changes in electrical resistance caused by volatile organic compounds; this data flows to collection stations where scientists can analyze the electrical signatures produced by the different compounds, identifying contaminants without having to transport actual water samples to the lab. The data can also be transmitted wirelessly to Web servers that would help spread the information to water safety officials around the country.

Ensuring that such information would

get to the people who can use it is a key part of efforts to shore up the infrastructure. And as one of eight areas singled out by the federal government's Critical Infrastructure Protection program—launched by President Bill Clinton in 1998 amid growing concerns about chemical, biological and computer-based attacks *(see "Partnerships to Improve Critical Infrastructures," p. 42)*—the nation's public water supplies will soon be linked to an Internet-accessible information-sharing and analysis center. Water utilities will pay a fee to join the exchange and use it to access and distribute data about contaminants found in the water supply as well as obtain intelligence reports from agencies monitoring terrorist threats.

The Washington, DC-based Association of Metropolitan Water Agencies, in charge of implementing the system, is patterning it after similar centers already operating in banking and finance and information technology. Other information-sharing systems are planned for transportation, telecommunications, emergency services, electric power and oil and gas distribution—all with the goal of giving government and private industry timely information about events disruptive to operations. "We've got to figure out how to get effective cooperation between local, state, federal and private organizations," says Randy Larsen, director of the ANSER Institute for Homeland Security, a nonprofit research organization in Arlington, VA, that consults with the government on national security issues. The centers, he says, mark a good start in that direction.

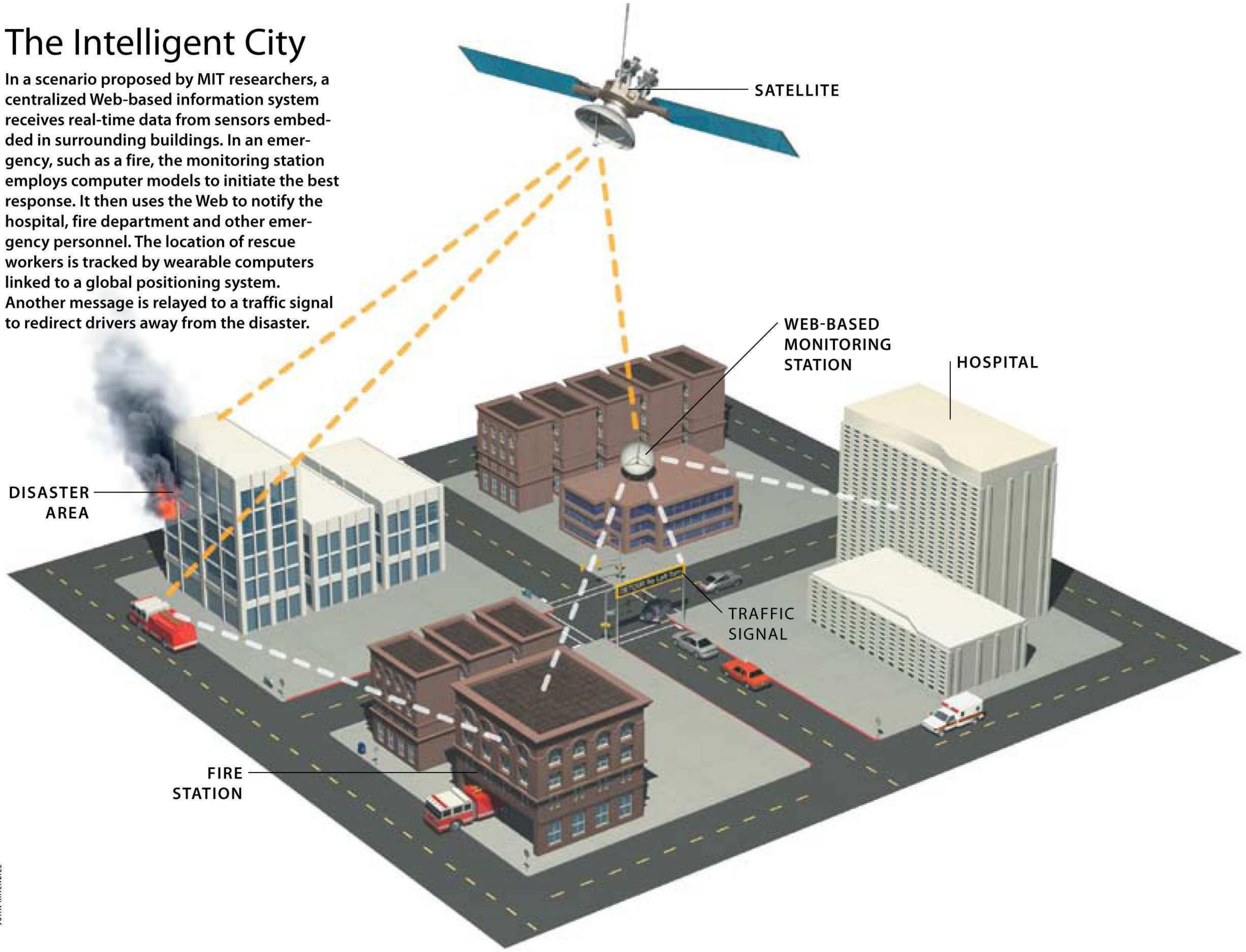
Cooperation and information sharing aren't all that's needed, however. Major parts of the infrastructure must be modernized so they can absorb and respond to disruptions more quickly and flexibly, observers say. The electrical grid, for example, needs new computerized controls to ensure that stresses on the system—whether in the form of a deliberate attack or simply a high-demand summer day—don't lead to widespread outages.

The problem isn't a lack of interconnections. While some power industry critics are calling for the construction of new transmission lines to add redundancy to the network, most regions of the nation already have several alternative paths for getting power from point A to point B. The real difficulty lies in controlling the flow of electricity. Today's power systems can't smoothly siphon electricity from overloaded lines to those with unused capacity, nor do they have any way of damping sudden disturbances such as voltage surges or selecting the best transmission path around a local outage. In short, as Lewis explains, the grid lacks the Internet's inherent resilience: "If part of the grid goes down, the rest of the system doesn't figure out how to route around it." And in an emergency, that means engineers must scramble to reroute power manually, either from a control center or by making manual adjustments to transformers in the field. "It's a dumb, antiquated system with no real architecture, so of course it's vulnerable to local attack," says McCarthy.

But here, too, help is on the way. Companies such as Siemens, ABB and Mitsubishi Electric are already testing new "power electronics" devices that can help automate the flow of electricity and smooth out unwanted fluctuations. One sophisticated switch, known as a gate turn-off thyristor, can detect lightning-speed spikes in power voltage and turn itself on and off fast enough to tame them and let controllers redirect excess power. Using these new power processors, which are being tested on key transmission lines that send power from upstate New York to Manhattan, engineers will be able to shunt power from one line to another at the touch of a button *(see "A Smarter Power Grid," TR July/August 2001)*. In emergency situations, the new devices should help grid managers switch seamlessly between primary and backup generating stations and transmission lines, minimizing the effects of attacks on individual facilities.

The Intelligent City

In a scenario proposed by MIT researchers, a centralized Web-based information system receives real-time data from sensors embedded in surrounding buildings. In an emergency, such as a fire, the monitoring station employs computer models to initiate the best response. It then uses the Web to notify the hospital, fire department and other emergency personnel. The location of rescue workers is tracked by wearable computers linked to a global positioning system. Another message is relayed to a traffic signal to redirect drivers away from the disaster.



JOHN MACNEILL

BUILDING THE I-CITY

Beefing up the interconnections of a city's utilities will go a long way toward making urban areas more resilient in the face of disaster. But what about strengthening the interconnections of the city itself? The same kind of redundancy and diversity found in the Internet, the water system and the power grid could be incorporated into city buildings and structures. Connecting those components electronically and then monitoring them could provide emergency-response crews with critical and timely information about any damage.

The system begins on the structural level with the buildings themselves. Additional support elements and secondary evacuation routes could help ensure that an event that compromises part of a structure doesn't lead to a catastrophic loss of life. Oral Buyukozturk, a professor in the MIT Department of Civil and Environmental Engineering, calls this principle "the technology of redundancy." Backup systems "should be incorporated into structures such that failure cannot be reached in one step," he explains. "Rather, it should take several steps."

While additional technologies such as stronger fireproofing might have delayed the accordion-like collapse of the World Trade Center towers, no one is suggesting that they could have prevented it. But the fact that few people escaped from offices above the stricken floors suggests that the airplane impacts did cut off most of the emergency stairwells in one step. And that, say Buyukozturk and others, brings the adequacy of tall-building evacuation systems into question. "We need better fire prevention methods and materials and better evacuation plans for tall buildings," Buyukozturk says. "The stairway should only be the first level of evacuation. The second level should perhaps be a special vertical tunnel or elevator, maybe installed in a tube made of a material such as reinforced concrete that is less affected by heat." Buyukozturk points to the pressurized service tunnel between the two railway tunnels under the English Channel as a working example. Thanks to the escape route the service tunnel provided, a November 1996 train-car fire that raged for nearly nine hours in one of the railway tunnels—causing considerable structural damage—killed no one.

When it comes to saving lives and stemming chaos in an emergency, it's also crucial that infrastructure managers are able to act intelligently. To do that, they need information. A growing number of engineers and city planners say the kind of intelligence exemplified by power electronics and the information-sharing and analysis centers should be woven through a structure's framework.

Researchers at Xerox's Palo Alto Research Center, for example, are proposing that legions of tiny, wirelessly interconnected sensors literally be mixed into building materials to provide a continuous report on a structure's physical state. "If you have sensors that are dirt-cheap and untethered—meaning they operate either on batteries or on passive energy that can be beamed to them—they could be blended into building materials such as concrete or brick," explains Feng Zhao, principal scientist of Xerox's Collaborative Sensemaking Project. "If each 'smart brick' has embedded sensors wirelessly communicating with other bricks, then during an emergency they can detect the extent of the damage."

Suppose a terrorist bomb blows a hole in a wall made from smart bricks or other networked materials. Some sensors would be knocked out of commission. But data collected from those that remained could allow structural engineers to quickly determine how big the hole is and how much stress has been placed on the remaining structure, explains Zhao. Even the demise of sensors could provide valuable information. "If these sensors are self-locating and part of the structure collapses, then as these bricks fall they are going to record and transmit their displacement," Zhao adds. "Maybe you can reconstruct their trajectories to see exactly how the building collapsed and where people might be trapped, and you can actually send rescue workers to the right place. That could be really useful."

Under more typical conditions, such sensor networks could be used to monitor the vibrations of passing vehicles or even footsteps, giving them obvious applications in the worlds of surveillance and military intelligence, which explains why Zhao's group is partly funded by the U.S. Defense Advanced Research Projects Agency. But Xerox's current prototype sensors range from a little larger than a quarter to the size of a shoebox, not quite small enough to incorporate into building materials. Zhao predicts it will take five to 10 years to make the hardware tiny enough and cheap enough—and suitably beef up the needed communications and data analysis software—to realize his vision. Nevertheless, he says his telephone has been "ringing off the hook" since September 11. "A lot of people think our sensor technology is right at the middle of making sure our cities are safer."

Indeed, such technologies could readily be adapted to monitor entire cities and coordinate disaster response, says Franz-Josef Ulm, a colleague of Buyukozturk in MIT's civil and environmental engineering department. "For about two years we've been discussing the concept of the 'I-City,' where basically you use monitoring and simulation of the physical state of the infrastructure—tunnels, bridges, buildings and so forth—to solve questions of the operations of the city," says Ulm *(see "The Intelligent City," p. 40)*.

One small test of the I-City idea is occurring on the MIT campus, where Ulm's students are wiring a flagpole with sensors that will monitor its temperature and movements caused by wind. The data will be sent to a server computer that displays the stats in real time on the Web. Meanwhile, simulation software will use the data to predict how much time remains until the flagpole fails from structural fatigue.

If these same kinds of sensors were sprinkled throughout a building's architecture, they could transmit the information upward from individual structures to the city monitoring station to a national anti-terrorism or disaster center. They could even be used to coordinate law enforcement and military responses. "How will we even know we are under attack in the 21st century?" asks the ANSER Institute's Larsen. "If you have an airplane crash in Chicago and the 911 system goes out in Sarasota and you have a big petroleum fire in Houston, are these just random acts? One of the things we need is a national command center, so we know an attack is going on, and that sort of real-time information is going to be very important."

A MEASURED RESPONSE

Because it's so difficult to know where terrorists will strike next, there is a natural impulse to retrofit as many components of the infrastructure as quickly as possible. But the resulting expense could be both crushing and ultimately futile, since terrorists might simply select targets that haven't yet been hardened. Most experts are therefore recommending a measured, planned approach to infrastructure protection, starting with a realistic look at threats and vulnerabilities. "We can't guard against every contingency, and there's no point in trying to do so," says policy analyst Peter Chalk, a specialist in national security and international terrorism issues at the Rand Corporation in Arlington, VA.

One prediction security experts can make is that the next attack probably won't resemble the last one. Thanks to heightened airport security and passenger awareness, for example, it's hard to imagine another attack using hijacked planes succeeding. "The plane as a delivery vehicle [for destructive energy] has been substantially abrogated just because of recent history," opines Exponent's McCarthy. But that doesn't mean landmarks like the Golden Gate Bridge are out of peril; indeed, notes McCarthy, there's a real threat to bridges and other structures in coastal cities from ships laden with explosive materials such as petrochemicals.

Foreseeing true threats and responding appropriately will require a new kind of thinking and a sustained sense of urgency, McCarthy and other experts say. As the immediate trauma of September 11 fades, there's a strong and understandable temptation to return to business as usual. But those who design, build and maintain the infrastructure are realizing that they must now make planning for the worst a part of their everyday work. TR

Partnerships to Improve Critical Infrastructures

INFRASTRUCTURE	FEDERAL AGENCY	PRIVATE INDUSTRY	PURPOSE OF PARTNERSHIP
Banking and finance	Department of the Treasury	Financial Services Information Sharing and Analysis Center	Provide members with early warnings about cyberattacks, such as the 1999 Melissa virus
Electric power	Department of Energy	North American Electric Reliability Council	Train utility employees to recognize and report suspected acts of physical or electronic sabotage
Emergency services			
> Fire and rescue	Federal Emergency Management Agency	National Fire Academy	Research fire-related threats, consult with and collect data from fire departments and publish information
> Law enforcement	Department of Justice, Federal Bureau of Investigation	National Communications System	Provide access to time-sensitive warnings of attacks on computing and communications infrastructure
> Public health	Department of Health and Human Services	To be determined	To be determined
Information technology	Department of Commerce	Information Technology Association of America	Build an online network for exchanging information about electronic threats and countermeasures
Telecommunications	Department of Commerce	National Coordinating Center for Telecommunications	Create and share electronic "event tickets" that contain information about vulnerabilities, threats and outages
Oil and gas	Department of Energy	National Petroleum Council	Create an information-sharing and analysis center
Transportation			
> Surface	Department of Transportation	Association of American Railroads	Set up an industry information-sharing and analysis center
> Air	Department of Transportation	To be determined	To be determined
Water	Environmental Protection Agency	Association of Metropolitan Water	Build an Internet-accessible center to broadcast alerts and information on vulnerabilities and crisis response

By Kevin Hogan   Illustration by Brian Cronin

Will Spyware Work?

Despite the most sophisticated intelligence-gathering technologies in the world, the United States failed to discover a band of terrorists that plotted within its borders. Will we miss them next time?

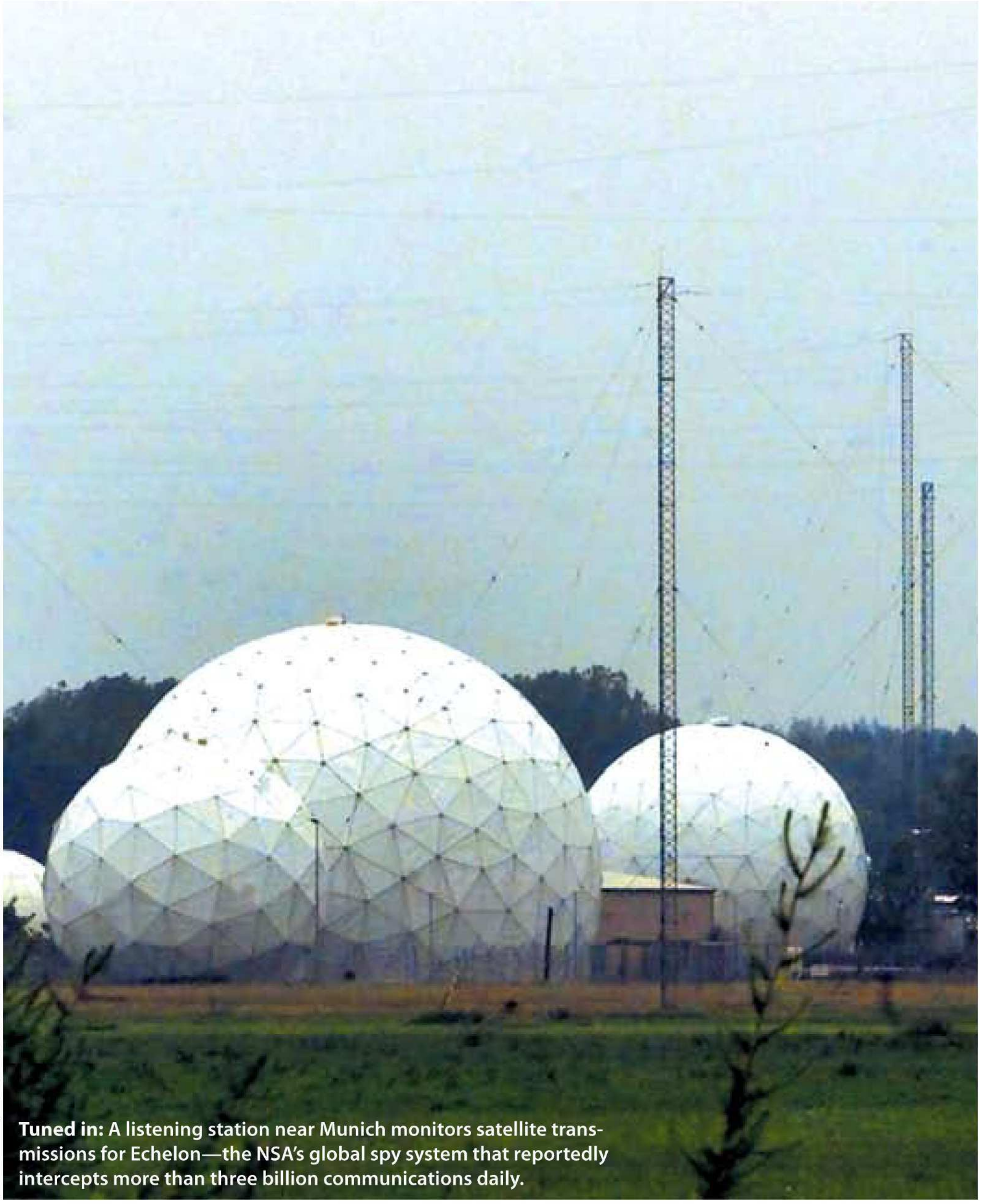
As the United States tries to grapple with the new realities of war and terrorism, questions for its intelligence community keep coming: How could something like September 11 occur without plans being detected? Who was tracking the activities of suspected terrorists inside the country? How were they even here in the first place? What happened to those high-tech, Big Brother-type surveillance tools like the notorious global-communications eavesdropping network Echelon, or Carnivore, the FBI's Internet snoopware, that were supposed to sniff out criminal activity?

For several decades, electronic systems have been quietly put in place to intercept satellite communications, tap phone calls, monitor e-mail and Web traffic and then turn this massive flow of information into intelligence reports for U.S. leaders and investigative aids for law enforcement. Yet despite the $30 billion

invested in them, and all the secrecy afforded them, government information technologies still could not connect the proverbial dots of the World Trade Center plot. "Obviously, there were intelligence failures on a number of levels," says Barry Posen, a defense policy analyst with MIT's Center for International Studies.

Now that it is apparent that these supposedly all-seeing government systems are not all-knowing, how can we ascertain that they work at all? While the technologies to intercept and capture any and every communication conjure images of an Orwellian omniscience (*see "Big Brother Logs On,"* TR *September 2001*), many experts say the ability to derive useful knowledge from all that data is still far from plausible. Even as the processing times get faster and the software gets smarter, the process of turning raw data into assured intelligence is far from perfect. If the goal is capturing, listening to and then actually sussing every single electronic communication in the United States, "In practical terms, we're not even close," says Gary McGraw, CTO at Cigital, a Dulles, VA-based network security software vendor.

It doesn't seem to be for lack of trying, however. Today, the U.S. intelligence community comprises more than a dozen major agencies, including the CIA, FBI and the National Security Agency. Within these bodies, there are dozens more departments, such as the CIA's directorate of science and technology, that specifically develop information technologies to aid in the practice of knowing what other people don't want them to know.


MICHAEL DALDER/REUTERS NEWS PICTURE SERVICE

Tuned in: A listening station near Munich monitors satellite transmissions for Echelon—the NSA's global spy system that reportedly intercepts more than three billion communications daily.

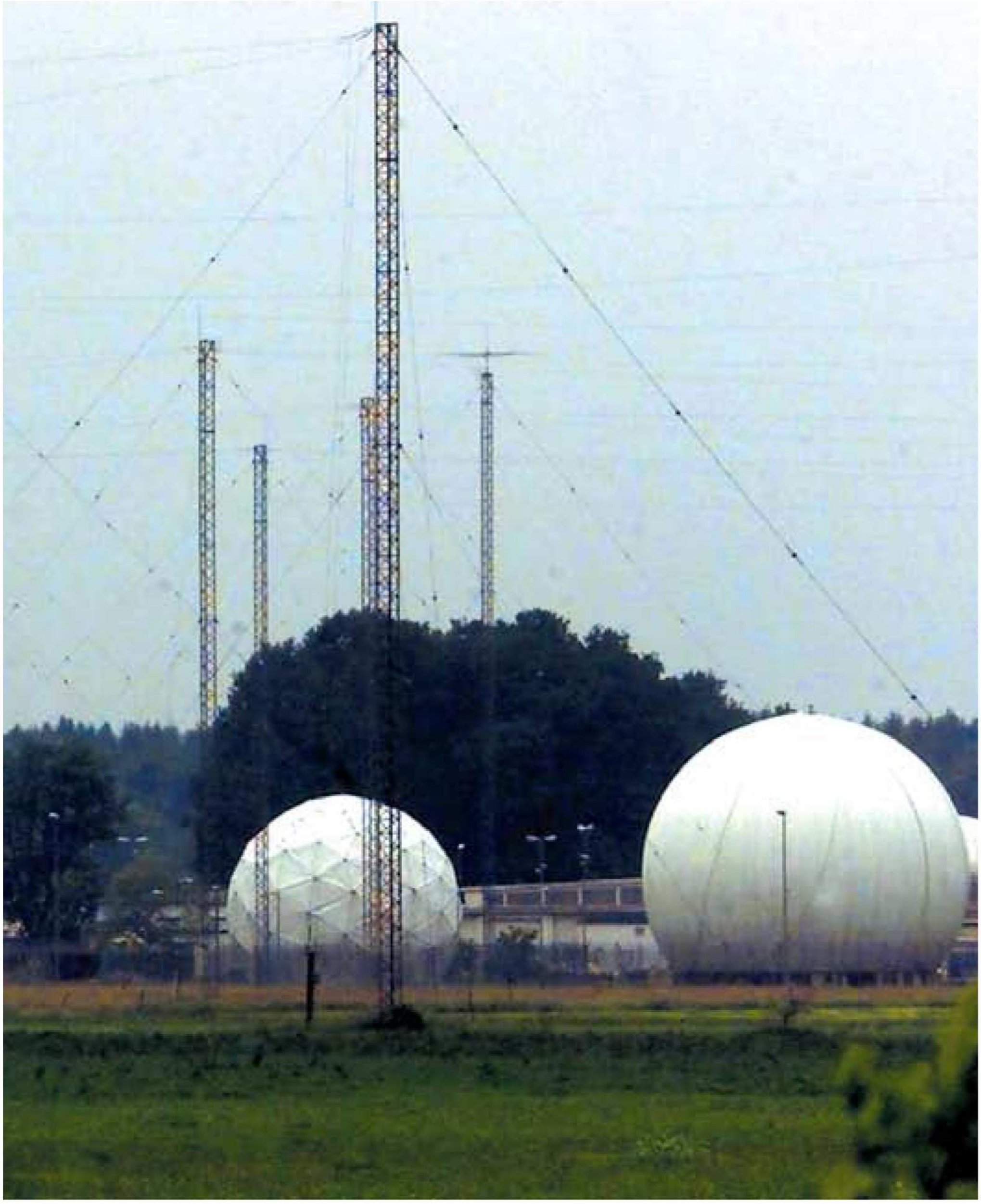
While the agencies theoretically cooperate, especially since September 11, there is no centralized information system to compare and contrast data collected among them. Critics claim that this bureaucratic and technical fragmentation is one reason terrorists were able to hatch their plan under the government's radar.

It is far from the only one. Even if intelligence agencies seamlessly integrate their knowledge, the tools available to them now and for the foreseeable future do not appear up to the task of providing the early warning needed to thwart terrorist plots. "My first reaction is not necessarily a question of why didn't these tools work, but how hard it would have been to discover this in the first place," says Sayan Chakraborty, vice president of engineering at Sigaba, a San Mateo, CA-based company specializing in e-mail encryption.

HEARING WITHOUT LISTENING

Despite its most recent, catastrophic lapses, the United States has a long and distinguished history of successfully using advanced information-gathering and analysis tools against its enemies. The Signals Intelligence Section, the forerunner of today's National Security Agency, came into being in World War II, when the United States broke the Japanese military code known as Purple and discovered plans to invade Midway Island. The NSA's early forays in cryptography contributed to the development of the first supercomputers and other information technologies. In his book *The Wizards of Langley: Inside the CIA's Directorate of Science and Technology*, National Security Archive senior fellow Jeffrey T. Richelson published more than 40 declassified documents that trace the CIA's exploitation of science and technology for the purposes of intelligence gathering. "From the early 1950s to the present, technology has played an essential part in analysis," he says.

The granddaddy of today's governmental electronic surveillance is Echelon, the National Security Agency's infamous,



NOW THAT IT IS APPARENT THAT THESE SURVEILLANCE SYSTEMS ARE NOT SO ALL-KNOWING, HOW CAN WE ASCERTAIN THAT THEY WORK AT ALL?

yet officially unacknowledged, global surveillance network. Said to be the most comprehensive and sophisticated signals intelligence setup in existence, Echelon reportedly has the capability to monitor every communication transmitted by satellite outside of U.S. borders—by some counts, three billion telephone calls, e-mail messages, faxes and broadcasts daily. Technically, Echelon technology could monitor domestic communications too, though that is prohibited under U.S. law.

According to a European Parliament report released in September, Echelon collects information through a complex web of radio antennae at listening stations across the planet. Other sources claim that one listening station in particular, at Menwith Hill in England, operated by U.S. and British intelligence services, is placed in the most convenient spot to tap transatlantic communications cables as well. Investigations cited by the American Civil Liberties Union and others report that Echelon rakes these immense volumes of data through "dictionary" software that operates on a vast computer network hosted by intelligence agencies from five countries—the United States, Britain, Australia, Canada and New Zealand. The dictionary program flags messages containing any of a set of predetermined keywords, such as "bomb" or "President Bush." The words are rumored to be changed on a regular basis.

How the actual process of data sifting works remains a mystery. National security restrictions prohibit anyone from speaking publicly about the program. Quips one source who has followed the technology, "Anyone who knows about it won't talk about it, and anyone who talks about it doesn't really know about it." Some experts suspect, however, that Echelon's data processing is based on a variety of technologies in use in the commercial world today, including speech recognition and word pattern finding. "Word pattern recognition is nothing new," says Winn Schwartau, a security consultant in Seminole, FL, and the author of *Information Warfare* and *Cybershock*. "We've been using that sort of stuff for years. But if you look at how advanced the searching abilities for the average person have become, I can only imagine the type of stuff that government security agencies have in operation."

According to Schwartau and others, the ability to sort through billions of messages and divine anything useful encompasses a number of techniques. Speech recognition systems and optical character readers convert spoken words (from phone conversations) and printed text (as from intercepted faxes) into catalogued and searchable digital data. Language translation software turns many of the world's spoken tongues into the English that the U.S. intelligence community prefers. Data-mining software searches volumes of data and establishes relationships among them by finding similarities and patterns.

Echelon has supposedly been using techniques like these to churn data into knowledge about foreign governments, corporations and even specific individuals since the 1970s. Subjects of surveillance are reported to have even included the likes of Princess Diana, whose work

eliminating land mines ran counter to U.S. policy. And in the months leading up to September 11, 2001, according to reports from the German newspaper *Frankfurter Allgemeine Zeitung*, snippets produced by Echelon intimated that "a big operation" was in place by terrorists seeking to destroy "American targets." Other information collected may in hindsight be pieced together to divine a much clearer picture of the operation. Unfortunately, things did not come together in time to warn of the attacks.

WATCH WHAT YOU TYPE

Another government snooping technology that has been the subject of controversy since long before September 11 is Carnivore. Comprising a set of programs in development by the FBI since 1996, Carnivore is devised to intercept data traffic sent over the Internet to assist federal authorities in criminal investigation. According to the FBI, Carnivore is installed only with the cooperation of an Internet service provider and after obtaining appropriate judicial approval to track e-mail, instant messages and Web search trails. And the system inspects only those communications that are legally authorized for interception.

That, at least, is the theory. Civil liberties organizations such as the ACLU, the Electronic Frontier Foundation and the Electronic Privacy Information Center worry Carnivore could be used to monitor much more than that.

To counter that suspicion, the U.S. Department of Justice hired Chicago-based IIT Research Institute to perform the only testing of Carnivore permitted outside government agencies. According to IIT's report, published last December, Carnivore works much like the commercial network diagnostic programs—called "sniffers"—that are used to monitor corporate networks, and runs on nothing more than an average personal computer.

After securing the proper warrants, the FBI will approach an Internet service provider to attach a Carnivore-loaded PC to its internal cabling. When plugged into a hub, the collection computer sees all data packets going by. It then copies only those packets that match settings prescribed by the FBI and approved by court order. Agents can view the captured packets in two different modes. In so-called pen mode, the system displays only information that identifies the sender and the intended recipient—numerical Internet addresses and e-mail names—and subject lines. In "full mode," the agent can access not just this address information but also the entire contents of the message.

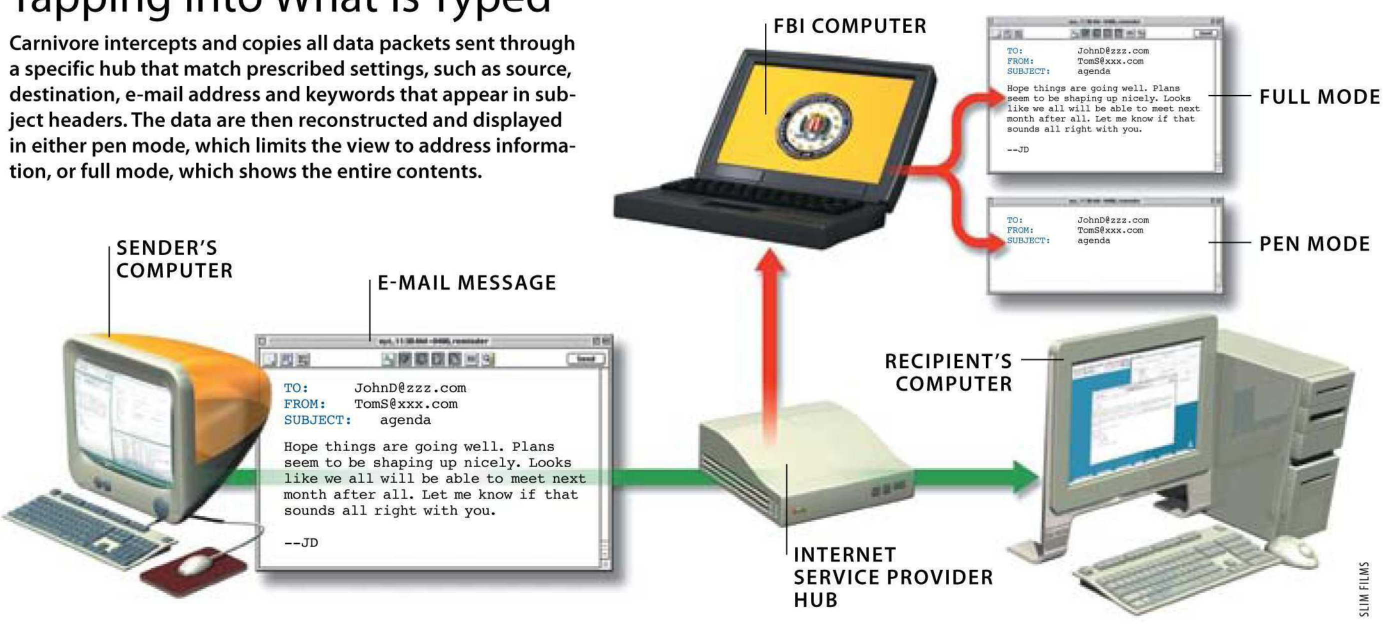
Once Carnivore has been installed at the Internet service provider, it is controlled remotely, according to the IIT report. The collection computer is connected to an analog voice line installed specifically for the particular tap. The intercepted data are stored on a two-gigabyte disk, which is then taken back to FBI laboratories for analysis. The data packets—broken bits of e-mail messages, Web pages and any other form of data sent across the Internet—can then be rebuilt and reviewed.

While Echelon and Carnivore are the most infamous intelligence collection tools, they are not the only ones, however. Government skunk works are constantly cooking up new tools to assist in covert surveillance operations. These include other quasi-legendary projects like Tempest, the code word for a number of surveillance technologies that can capture data displayed on computer screens by picking up electromagnetic emissions from the internal electron beams that create the images.

Every once in a while, the intelligence community opens its cloak to show off some of its tricks. Last March, for example, Larry Fairchild, director of the CIA's office of advanced information technology, brought a group of reporters into the basement of the agency's headquarters in Langley, VA. There, he demonstrated two programs deemed safe for public consumption: Fluent and Oasis.

Tapping into What Is Typed

Carnivore intercepts and copies all data packets sent through a specific hub that match prescribed settings, such as source, destination, e-mail address and keywords that appear in subject headers. The data are then reconstructed and displayed in either pen mode, which limits the view to address information, or full mode, which shows the entire contents.



Fluent performs computer searches of documents written in different languages. An analyst types in a query in English, just as if he or she were using a garden-variety search engine like Google. The software fishes out relevant documents in a number of foreign languages—including Russian, Chinese, Portuguese, Serbo-Croatian, Korean and Ukrainian—and then translates them into English.

Oasis converts audio signals from television and radio broadcasts, such as those from Qatar-based al-Jazeera, into text. It distinguishes accents, whether the speaker is male or female, and whether one voice is different from another of the same gender. The software then generates a transcript of those transmissions, identifying which voice uttered which statements. While Oasis can today comprehend only English-language programs, the CIA is developing versions that work in Chinese and Arabic, among other languages. Oasis can reportedly process and analyze a half-hour broadcast in as little as 10 minutes, as opposed to the 90 minutes that the task typically takes for an analyst working without the software.

EVEN THE MOST ADVANCED SPYING TECHNOLOGY CAN BE STYMIED BY COUNTERMEASURES THAT ARE EMBARRASSINGLY PRIMITIVE.

FUTURE FUTILITY

Assuming all this impressive high-tech wizardry is fully operational, how could a band of terrorists, including many already suspected as such, operate within U.S. borders for years and still escape detection—undoubtedly making phone calls and exchanging e-mail with coconspirators all the while? The answers, unfortunately, don't provide a basis for optimism about the ability of these systems to offer much protection in the new war against terrorism.

First, security and intelligence experts agree that the mass of information generated every day around the world far outstrips the capacity of present-day technologies to process it. "You're talking about incredible mountains of information, and trying to find that needle," says McGraw.

Intelligence agency leaders themselves have admitted their vulnerabilities. "We're behind the curve in keeping up with the global telecommunications revolution," National Security Agency director Michael Hayden told CBS's *60 Minutes* in a rare public admission last February. In testimony to Congress days after the attacks on the World Trade Center and Pentagon, Attorney General John Ashcroft warned that terrorists still have the "competitive advantage" when it comes to domestic espionage, and that "we are sending our troops into the modern field of battle with antique weapons."

Then there is the matter of encryption technologies that can turn even intercepted communications into gobbledygook. "The odds are nigh on impossible that the NSA or anybody else is going to be able to break" an encrypted message, says security expert and author Schwartau. Another technology that Osama bin Laden's minions reportedly used falls under the rubric of steganography: cloaking one type of data file within another. It is possible, for example, to hide a text file with attack plans within a bit-mapped photo of Britney Spears. Just try to filter down the number of those images flying around the Internet.

And even the most advanced spying technology can be stymied by embarrassingly primitive countermeasures. Conspirators can go the old-fashioned route of disguising their activities by using simple ciphers that substitute letters for numbers or other letters; Thomas Jefferson used such codes in his international communiqués as George Washington's secretary of state. Cigital's McGraw says this would be the easiest way to avoid detection: "To use a crude example: maybe the terrorists substituted the word 'banana' for 'bomb' and 'orange' for 'World Trade Center.' Do you flag every unusual pattern with random associations?"

Beyond the pure technology issues lies the question of how these tools can be used in a way that is compatible with an open and democratic society. Even in the rally-round-the-flag mood following the attacks, many U.S. citizens expressed concern about the government's expanding authority to snoop on their movements and communications. Organizations like the Electronic Frontier Foundation are highly vigilant about governmental attempts to expand the use of surveillance technologies such as Carnivore. "We really have no sense beyond a few basics they decided to reveal about how they use these tools," says Lee Tien, senior staff attorney for the organization. "They just want us to accept that they need them, without explaining why or how."

And while technologies like Carnivore have proved useful in investigations of specific individuals, they could be abused when directed at wider groups. People can quickly become "suspects" on no more evidence than an e-mail received or a Web site visited.

In the end, computer-based surveillance technologies may be best employed after the fact, says John Pike, director of GlobalSecurity.org, a Web-based military and intelligence policy group headquartered in Alexandria, VA. He notes that Carnivore, in particular, "was very effective in tracking down" and arresting former FBI agent and Soviet spy Robert Hanssen. "It also helped dramatically after the bombing to track down these terrorists' activities. It helped them detain at least 400 to 500 other people as suspects." According to Pike, U.S. citizens are going to have to become comfortable with such mass arrests if this type of technology is going to be used.

Even if the obstacles of bureaucracy, societal resistance and technical limitations were all to be surmounted, there's no assurance that high-tech spyware would ever provide the kind of security that people now crave. Will these technologies help recognize the danger next time? Even the most sophisticated intelligence paraphernalia still can't guarantee success when pitted against the malevolent combination of human ingenuity and capacity for evil. TR

By Alexandra Stikeman

Recognizing the Enemy

Face recognition technology could soon become an integral part of security systems.

AP PHOTO/PORTLAND POLICE DEPARTMENT (SURVEILLANCE); AP PHOTO (ATTA); FACIAL FEATURE ANALYSIS COURTESY OF VISIONICS

Facing terror: Security camera images like that of Mohamed Atta in a Maine airport (left) could be matched to images of suspected terrorists on file with authorities, using face recognition technology that measures facial features like those indicated on Atta's driver's-license photo (right).

Of all the dramatic images to emerge in the hours and days following the September 11 attacks, one of the most haunting was a frame from a surveillance-camera video capturing the face of suspected hijacker Mohamed Atta as he passed through an airport metal detector in Portland, ME. Even more chilling to many security experts is the fact that, had the right technology been in place, an image like that might have helped avert the attacks. According to experts, face recognition technology that's already commercially available could have instantly checked the image against photos of suspected terrorists on file with the FBI and other authorities. If a match had been made, the system could have sounded the alarm before the suspect boarded his flight.

In the wake of the attacks, a number of companies, security professionals and government officials have proposed using biometrics—identification based on a person's unique physical characteristics—to enhance airport security. "We've developed some fantastic technologies, but we just haven't deployed them," says Georgia State University aviation safety researcher Rick Charles. Readily available biometric techniques include digital fingerprinting, iris scanning, voice recognition and face recognition.

Of these technologies, face recognition is perhaps the best suited to surveillance of busy public places like airports. For one thing, it doesn't require those being watched to cooperate by looking into an iris scanner or putting a hand on a fingerprint reader; face recognition devices can work with the video feeds from the cameras that are already ubiquitous in public spaces. It's also much easier for authorities to obtain a suspect's photo—from a passport or driver's license, for example—than it is to obtain other biometric identifiers.

Indeed, many government agencies, from the FBI and the CIA to the Immigration and Naturalization Service and the Drug Enforcement Agency, keep large databases of photos. When the FBI places a suspected terrorist on a watch list, the agency circulates that person's photo to local police, immigration officers or customs agents. "But if you're a cop, you've got to be pretty good at quickly scanning faces in a crowd [for terrorists]," says Richard Norton, executive director of the International Biometric Industry Association. With face recognition technology, security officials could link their surveillance cameras to any number of databases via the Internet and let a computer do all the work, alerting officials when it finds a positive match.

Setting up a face-recognition-based security system would be relatively simple. The two major players in the area of face recognition, Littleton, MA's Viisage Technology and Visionics in Jersey City, NJ, say they have systems that could easily do the job. Visionics' device plugs into a video camera and grabs images of faces while the camera is recording. Software extracts the unique characteristics of each face and creates a template, a compressed digital file that can then be sent over the Internet to several databases at once. Further Visionics software installed alongside each database sifts through a million photos per second and signals when it finds a match.

In essence, all the elements needed to create a wide-scale security system based on face recognition are already available.

But to implement such a system could be a bureaucratic nightmare, requiring the cooperation of multiple federal and local authorities. Each agency would have to allow access to its photo databases from different security checkpoints throughout the country. "That's going to require some federal decisions on how that information is shared," says Norton. "That process is under way. These issues are being discussed at the relevant agencies."

Federal officials could not be reached for comment on the status of these discussions. But face recognition was one of a number of new security measures that the U.S. Department of Transportation explored after the attacks. In late September, Visionics CEO Joseph Atick demonstrated his company's technology to an emergency committee set up by the department. In its final report, the committee recommended that airports implement biometric technologies, though it did not specify which ones. But according to committee member Charles Barclay, president of the American Association of Airport Executives, "Face recognition definitely has a future in airport security and air transportation." In fact, officials at the Massachusetts Port Authority, which manages Boston's Logan Airport, revealed in October that they had independently made plans to begin using face recognition at Logan by the end of the year.

Airport security, however, could be just one part of a wider antiterrorism system using face recognition. The technology could potentially be employed at government buildings, embassies, border crossings and large public events.

In his briefing to the special transportation committee, Atick went so far as to outline what he refers to as a four-layer "national shield." The first layer would use face recognition as part of the visa application process, checking each applicant's photo against databases of known and suspected terrorists. "This is to keep terrorists at home," Atick says. "Don't bring them into the United States by offering them visas." The Immigration and Naturalization Service and the State Department could also prevent some forms of identify fraud by making sure an individual doesn't apply for a visa multiple times under different names. Three other layers of security would be created by installing face recognition technology at airport ticket counters, metal detectors and boarding gates, all linked to the same databases. This setup would ensure, according to Atick, that no suspected terrorist obtains a boarding pass, and that legitimately obtained boarding passes don't fall into terrorists' hands.

THE TECHNOLOGY IS READY TO GO, BUT IMPLEMENTING A NATIONWIDE FACE RECOGNITION SYSTEM COULD BE A BUREAUCRATIC NIGHTMARE.

Even before the September 11 attacks, the U.S. Defense Advanced Research Projects Agency (DARPA) had begun its own research efforts in face recognition and other biometric technologies. Indeed, face recognition is a key part of DARPA's four-year, $50 million "Human ID at a Distance" project, launched in February 2000 to develop a sophisticated surveillance system for U.S. embassies and facilities at home and abroad *(see "Big Brother Logs On,"* TR *September 2001)*. The system would combine cameras, radar and various types of sensors to identify people up to 150 meters away not only by their faces, but also by the way they walk, for example, or measurements like girth and leg length. The project not only illustrates the government's intense interest in using biometrics to enhance national security, but could also serve as a window into the highly sophisticated systems that might be used in the future.

As promising as face recognition and other biometric technologies look, though, one overriding caveat remains. Simply put, to use biometrics to catch bad guys, you have to start with some idea of who the bad guys are. Surveillance cameras could check each face in an airport against the FBI's database, for example, but if the agency hadn't turned up the fact that the man at the coffee stand in the blue coat had trained at an al-Qaeda camp, and his photograph wasn't in its database, the check would have done no good. It's still unclear, in fact, whether the FBI had Atta's picture on file before the September 11 attacks. In other words, biometric data would have to be supported by good intelligence to be a powerful weapon in the battle against terrorism. TR

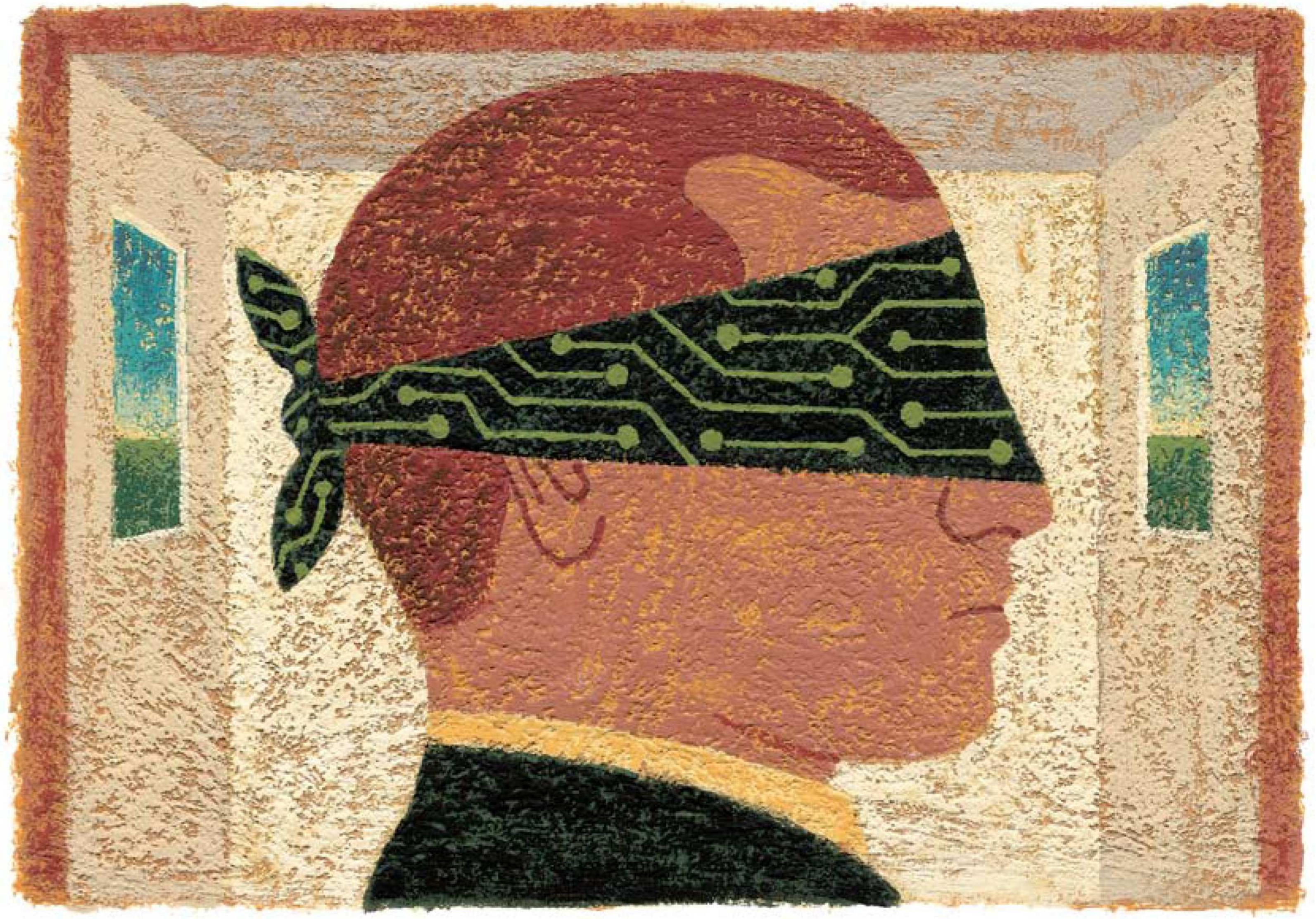
Companies Eyeing Large-Scale Applications of Biometrics

COMPANY	TECHNOLOGY	WHERE	PURPOSE
EyeTicket **McLean, VA**	Iris recognition	Heathrow Airport, London	Speed passenger check-ins
Recognition Systems **Campbell, CA**	Hand geometry	Eight major airports in North America	Speed immigration clearance for international travelers
Viisage Technology **Littleton, MA**	Face recognition	More than 100 casinos worldwide	Identify known casino cheats and reduce fraud
Visionics **Jersey City, NJ**	Face recognition	London and Birmingham, England	Detect known criminals and deter crime
Visionics **Jersey City, NJ**	Face recognition	Mexico	Eliminate duplicate voter registrations

By Edward Tenner Illustration by James Steinberg

The Shock of the Old

Our focus on new technology, as both the source of our vulnerabilities and the answer to our problems, can go too far.



On September 11, when terrorists forcibly diverted two airline flights into the twin towers of the World Trade Center and a third plowed into the Pentagon, stunned surprise and inconsolable grief could be our only initial response. Then came an apprehension that will long be with us: how many other terrorist cells are still out there, and will we be able to find them in time?

But to many of those who have followed the scientific and technical side of warfare and terrorism, there was yet another jolt. It was comparable to the horror of the military analysts in December 1941 who had been expecting a Japanese preemptive strike in the Philippines or elsewhere in Asia, but not at Pearl Harbor. Assumptions were fatally wrong. Things were not supposed to be this way. We faced an old nightmare, not the futuristic dystopia of information warfare and massive chemical or biological attack that we had dreaded.

In the 1990s, as advanced systems triumphed in the Gulf War and the Nasdaq index began to soar, conflict was supposed to be going high tech. In December 1995, for example, a dozen Marine Corps generals and colonels, including the commandant, General Charles Krulak, visited the World Trade Center. They were studying how to master information overload by observing some of the top traders of the New York Mercantile Exchange practicing simulated commodity activity. Later, they conducted simulated combat exercises with 15 traders at advanced workstations on Governor's Island off the southern tip of Manhattan. How could the images on those 69-centimeter monitors have warned them that less than six years later, the Twin Towers would become the battleground of a domestically launched air war?

Of course we feared attacks from the Middle East and elsewhere in the late 1990s. But the bad guys, we thought, were getting online, just like us. As the year 2000 approached, military and civilian authorities were on high alert, not only for accidental failures of vital systems but for cyberattacks using the date change as a smoke screen. Yet the nation's pipelines and electrical grids survived the new year without incident. Even the powerful anti-U.S. emotions of the Kosovo war produced no serious assault on the U.S. infrastructure. Only too late did we realize what a cataclysm had been in preparation.

Our tragic mistake was not that we pursued the new. It was that we neglected the old. And it's a pattern that could have troubling implications if we don't recognize its applicability to other key parts of our technological culture.

In the case of the September 11 attacks, as journalists soon realized, the terrorists' methods were surprisingly low tech. In fact, the technologies involved had been established for a generation—30 years, plus or minus five.

While the building design was tested to withstand a hit from a 707 jet, the Boeing 747, with its immense fuel loads, was already in service by 1969. The terrorists also apparently needed no sophisticated knowledge of automatic pilots and global positioning satellites. They had simply, and all too well, learned the classic principles of flying.

The immediate goal of the hijackers was also a 1970s concept: stunning the world with photogenic violence, as at the 1972 Munich Olympics. Thanks to satellite feeds, cheap color televisions and the Internet, these images could now have a more rapid and vivid impact, but the principle was old hat. So was the idea, dating at least from the time of the Ho Chi Minh sandal—carved by resourceful Viet Cong soldiers from rubber tire segments—that the improvised technologies of poor countries and peoples might humiliate the West. The terrorists understood all too well this neglected feature of technology: with enough determination, practice and time, mature and even seemingly outdated tactics and devices can be reborn.

What can halt future attacks? The events showed the limits of communications monitoring and satellite surveillance. The question remains whether more ambitious programs like the FBI's troubled Carnivore e-mail-sniffing technology or facial recognition software will unearth new data on terrorist activity, or simply compound the familiar problem of information overload and produce an illusion of control. The frequent false alarms from even the simplest home security systems are already a plague for the police.

We obviously need to think more about protection from both newer and older forms of attack. One common feature of both is reliance on personal networks. The terrorist cells' apparent methods of recruiting from the same regions, clans and families, and moving frequently from base to base, make them difficult to infiltrate conventionally—but they also reveal patterns to experienced analysts, making more targeted technical surveillance possible. We don't need another decimal place of accuracy from computational social-science studies but a better intuitive understanding of the terrorists and their civilian neighbors. At the same time, the tacit knowledge possessed by the most effective police officers and detectives deserves more respect. One of our great challenges will be to formalize and teach these elusive skills to security screeners at airports and elsewhere.

THE SHOCK OF THE OLD IS NOT LIMITED TO BREACHES OF NATIONAL SECURITY. MANY PROFESSIONS ARE LOSING THEIR TECHNOLOGICAL BALANCE.

But the shock of the old is not limited to breaches of national security. The civil engineer and historian Henry Petroski, in his book *Engineers of Dreams: Great Bridge Builders and the Spanning of America*, points to a 30-year cycle in which a new generation of professionals forgets the hard-won lessons of its predecessors' errors. Indeed, there are signs that many professions have started to lose their technological balance. Many U.S. medical residents, for example, are no longer highly skilled in using a stethoscope to interpret body sounds. The demands of training physicians for tomorrow's biotechnology may be in conflict with the best preparation for hands-on contact with today's patients. Doctors obviously need to know the latest science, but both educational trends and the pressures of managed care make it harder for them to read facial expressions alongside lab reports.

What makes a good lawyer, too, is not just access to databases of legislation and decisions but intuitive knowledge of clients and clients' environments. That's why most lawyers still avoid representing themselves despite all the new tools at their disposal. They're paying not for formal information but for tacit knowledge.

Librarians tell me that students often spend much more time finding certain information on the Web than they would have needed using standard printed reference books. Internet skills are indispensable—in fact, they too are not taught enough—but so is the ability to access the vast body of essential knowledge that has not been and may never be available in an electronic format. The high cost of both electronic and paper information, not to mention terminals and printers, challenges librarians, but most of them recognize that each mode has irreplaceable advantages.

In fact, engineering itself is not just the application of mathematical equations but a subtle balance of aesthetics, economics and science in which culture counts as much as calculation. Computer-assisted design can accelerate execution of ideas but can never replace the insight that comes from immersion in the traditions of building. It was the cultural resonance of towers and polygons, used by brilliant designers, that made the targets of September 11 such powerful icons, not simply their acres of usable space.

Just as the Nasdaq's collapse well before September 11 was a symptom of an economy out of balance, so this infinitely greater catastrophe reminds us to seek a new equilibrium between virtual reality and the real kind, between pixels and iron and concrete, flesh and blood. As Dan Rather told his viewers during the ordeal, "This is not a graphic." TR

Edward Tenner is a visiting researcher in the Princeton University Department of English and author of Why Things Bite Back: Technology and the Revenge of Unintended Consequences *(Vintage Books).*

Join an online discussion of this article at www.technologyreview.com/forums/antiterrorism

Game, set, match: Chief scientist David Gelernter of Mirror Worlds Technologies says the desktop metaphor is over.

WORTH

THE NEXT COMPUTER INTERFACE

The familiar "desktop" we use to operate our PCs is obsolete. New on-screen metaphors that take advantage of our sense of time and space are on the way.

"The desktop is dead," declares David Gelernter. Gelernter is referring to the "desktop *metaphor*"—the term frequently used for the hierarchical system of files, folders and icons that we use to manage information stored on our home or office computers. At the annual gathering of technophiles at TechXNY/PC Expo 2001 in New York last June, he told the rapt crowd attending his keynote speech that the desktop metaphor is nothing more than virtual Tupperware. "Our electronic documents are scattered by the thousands in all sorts of little containers all over the place," he said. "The more information and the more computers in our lives, the more of a nuisance this system becomes."

For the past decade or so Gelernter has been campaigning for a new metaphor to overthrow the desktop—first in research he carried out at Yale University, where he is a professor of computer science, and now as chief scientist of his new company, Mirror Worlds Technologies, with offices in New Haven, CT, and New York City. In March, Mirror Worlds announced a novel metaphor called Scopeware, software that automatically arranges your computer files in chronological order and displays them on your monitor with the most recent files featured prominently in the foreground.

By Claire Tristram | Photographs by Timothy Archibald and Jonathan Worth

Scopeware is far more sweeping than a simple rearrangement of icons, however: in effect, it transfers the role of file clerk from you to the computer, seamlessly ordering documents of all sorts into convenient, time-stamped files.

If you have ever forgotten what you named a file or which folder you put it in, you probably will agree that it's time for a change. The desktop metaphor is decades old, arising from early-1970s work at Xerox's fabled Palo Alto Research Center, and was never intended to address today's computing needs. Indeed, the product that brought the metaphor to mass-market attention was Apple Computer's 1984 Macintosh; it had no built-in hard drive, and its floppy disks each stored only 400 kilobytes of information. Today we're using the same metaphor to manage the countless files on our ever more capacious hard drives, as well as to access the virtually limitless information on the Web. The result? Big, messy hierarchies of folders. Favorites lists where you never find anything again. Pull-down menus too long to make sense of.

In other words, the desktop metaphor puts the onus on our brains to juggle this expanding collection of files, folders and lists. Yet "our neurons do not fire faster, our memory doesn't increase in capacity and we do not learn to think faster as time progresses," notes Bill Buxton, chief scientist of Alias/Wavefront, a leading maker of graphic-design tools. Buxton argues that without better tools to exploit the immense processing power of today's computers, that power is not much good to us.

That's why many researchers—at universities and startups like Gelernter's Mirror Worlds as well as giants like Microsoft and IBM—are searching for alternatives. They're examining metaphors taken from other media, such as books or diaries or film; 3-D schemes that use our sense of spatial orientation to create the illusion of depth on-screen, so that documents look closer or farther away depending on their importance to us; alternatives that borrow from video games the notion of having an intelligent guide, or avatar, to help us find what we're looking for; or even theories that radically change the notion of what a "computer" is, so that we no longer think of devices as computers at all and are therefore open to new ways of interacting with them.

"The desktop metaphor made assumptions about how we use computers that just aren't true anymore," asserts Don Norman, cofounder of the Nielsen Norman Group, famed critic of computer design and author of *The Design of Everyday Things*. "It's time to throw away the old model."

Learning Esperanto

It will take a Herculean effort to overthrow the desktop metaphor—many observers believe it will prove impossible—chiefly because the three-decade-old interface, popularized by the Mac and quickly made nearly ubiquitous by Microsoft's Windows, has become integral to our very notion of personal computing. "A couple of years ago we did a study on how to introduce new computing models," says Dan Russell, research director in the field of human-computer interaction at the IBM Almaden Research Center in San Jose, CA. "We wanted to find people who didn't understand the function of file folders, how to open files, how to delete files. We couldn't find anyone. That makes it hard to change people's expectations of how computers should behave."

With this in mind, looking over the landscape of alternatives, one comes away wondering if the desktop metaphor has become a part of basic cultural literacy, like language itself, and that getting people to try any of the suggested improvements is like getting them to learn an international language like Esperanto—a good idea in theory, but for most people not worth the trouble.

Even its biggest critics today acknowledge that the desktop metaphor was an extraordinary breakthrough that tapped into the way people actually work and think, a vast improvement over typing in text commands alongside a blinking cursor. Still, people like Gelernter remain undaunted in their belief that its moment has passed. "It was a brilliant idea at the time," he says. "But it's explicitly tied to the way we managed information in the 1940s, with filing cabinets filled with separate folders of information. Even 10 years ago the notion of putting stuff in files and sticking certain files in folders and others on your desktop was already broken down and failing."

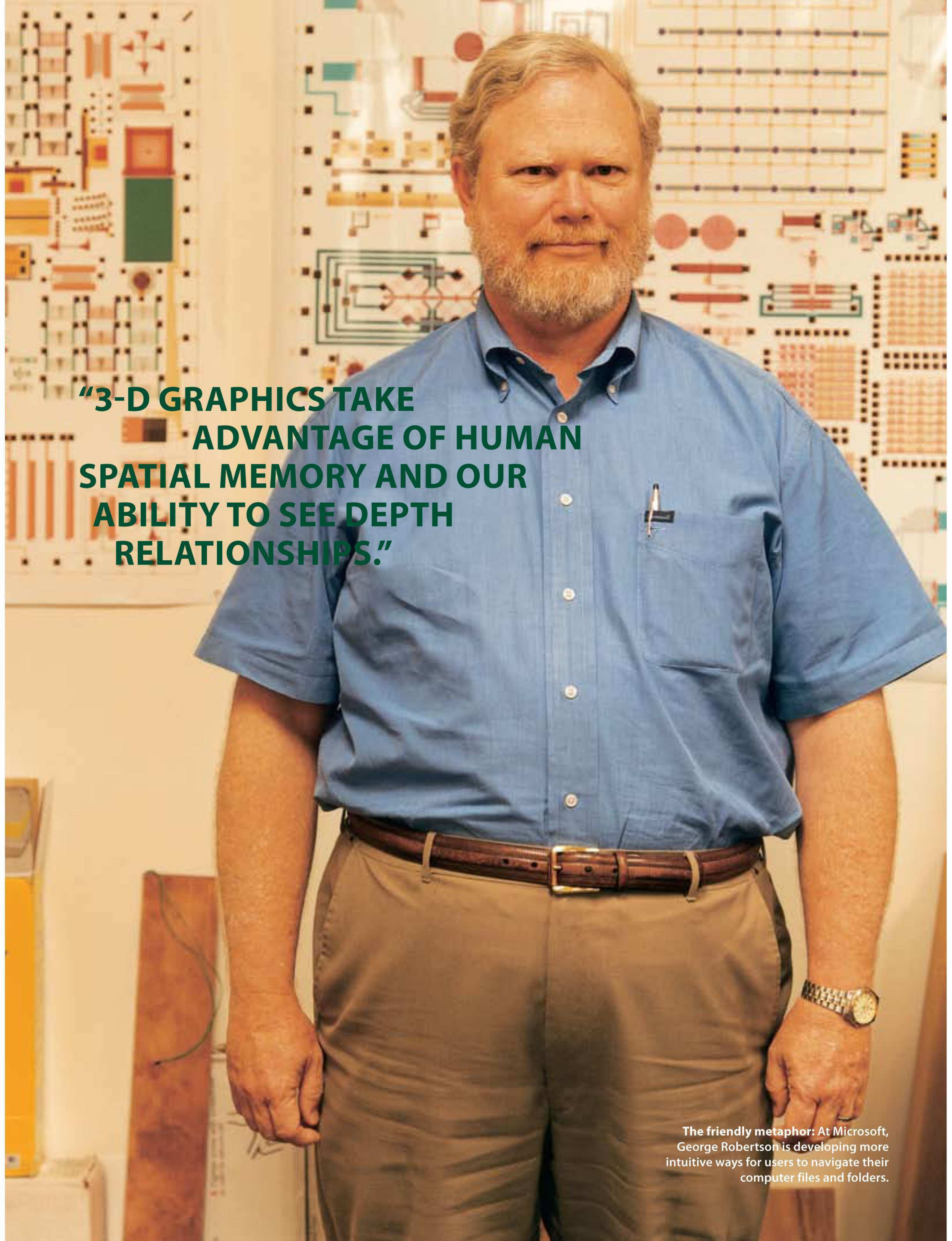
Gelernter's alternative, Scopeware, is the outcome of a decade of research and development at Yale. Scopeware replaces the desktop metaphor with what Gelernter calls a "narrative information system," or what you might call the diary metaphor, where every type of file—an e-mail message, a word processing document, a digital image—is stored chronologically, in what appears on-screen to be a tiling stack of file cards *(see Scopeware screen shot, p. 56)*.

Search for the term "demo" on the Mirror Worlds Web site, for example, and you get a stack of six virtual file cards, dated back to February 9, 1998. In the upper right-hand corner of each card you see an icon indicating the type of file—in this case, four files in Adobe Acrobat, one in Microsoft Word and one in Microsoft's Internet Explorer that was taken from a Web page. On each card you see the title of the file, plus a small box previewing what's inside. Moving your mouse's pointer over one of the cards brings up a summary of the document and a larger picture, so you can see if it's what you want; a double click opens the file itself. Search for "Gelernter" and you get about 70 such cards, chronologically arranged, with older documents receding into the background. You know immediately how to navigate. Scopeware works.

The diary metaphor has some clear advantages over the desktop metaphor. It is based on the notion that what we have created, modified or even looked at most recently is probably still most important to us. And, Scopeware's inventor maintains, our sense of time is a strong organizing principle that can help us locate a file simply because we remember when we used it last. Rather than requiring you to manually rifle through buckets of information stored on your hard drive or inside an application like e-mail, Scopeware sorts information automatically, streaming it into predetermined categories.

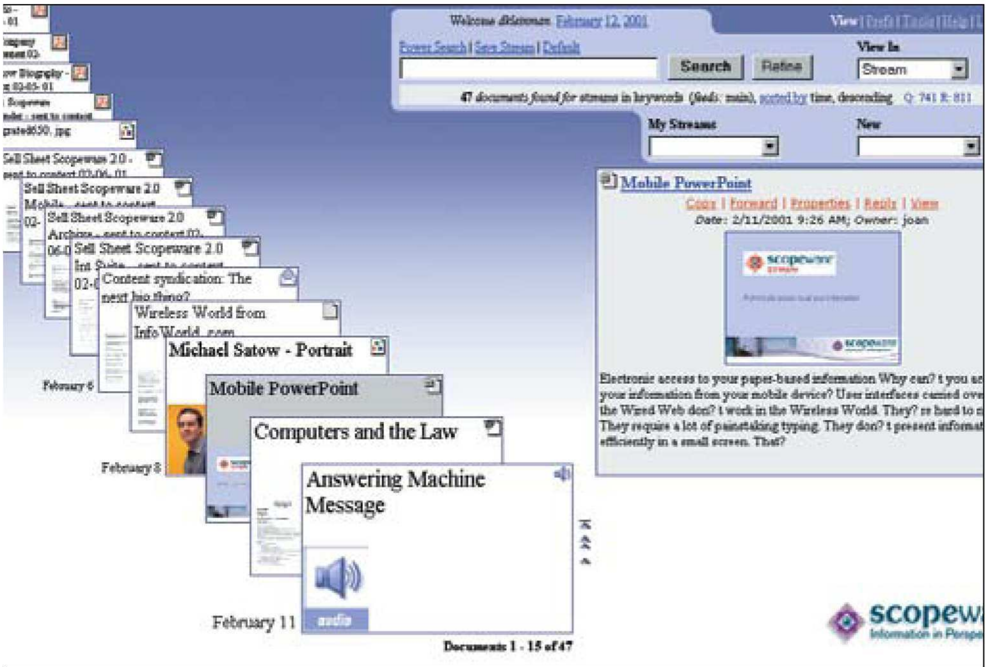
But kill the desktop? While Gelernter has deeply criticized the desktop metaphor in his books and in a manifesto about the future of digital technology called *The Second Coming*, it's our years of familiarity with that Xerox PARC design—the point and click, the icons and the menus—that make Scopeware so intuitive. Those of us who were 15 or older when we used our first mouse still remember how difficult it was, initially, to equate the horizontal movement of our mousing hand with the movement of the cursor on-screen. Now it's natural. And

ARCHIBALD

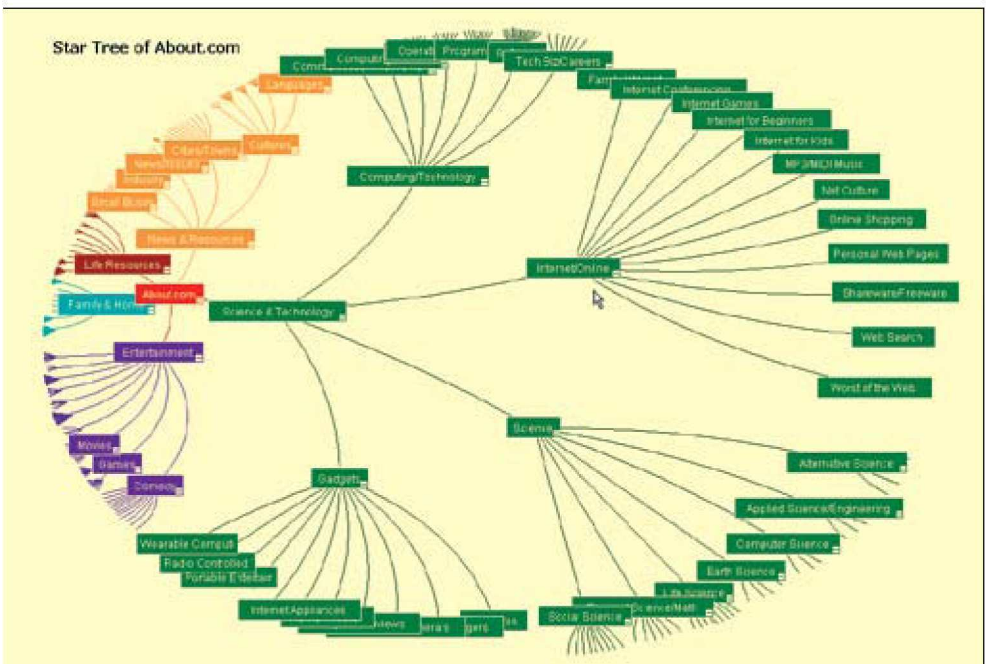


“3-D GRAPHICS TAKE ADVANTAGE OF HUMAN SPATIAL MEMORY AND OUR ABILITY TO SEE DEPTH RELATIONSHIPS.”

The friendly metaphor: At Microsoft, George Robertson is developing more intuitive ways for users to navigate their computer files and folders.



COURTESY OF MIRROR WORLDS



COURTESY OF INXIGHT

Order amid chaos: Mirror Worlds' Scopeware (top) automatically streams files into preset categories and displays them in an easy-to-navigate fashion. Star Tree (bottom), developed by Inxight, organizes hierarchies of files and folders around a sphere that users can rotate.

Scopeware, if it succeeds, will do so because it makes use of what we already have. The company has positioned the product as a business software tool that helps companies organize and share information, rather than as a replacement for Windows; it works through a browser rather than as an operating system. "We aren't taking on Windows at all," Gelernter says. "That would be suicidal."

That's the quandary that researchers in the field of human-computer interaction have long struggled with: make something look too different on-screen, however good it is, and you will fail. "About ten years ago I realized that I wasn't able to say, 'Okay, turn off your machine, because tomorrow I'm going to bring you a brave new world,'" says Ramana Rao, a founder of Inxight Software, a Santa Clara, CA-based startup funded by Xerox that is also exploring and marketing new user interfaces. "I needed to accept that there are hundreds of millions of PCs out there, and figure out where within that structure I could insert the thin edge of a wedge of a new way of doing things, where I could show you something incrementally better, then start pounding on the wedge until the old face drops away."

Like Mirror Worlds, Inxight doesn't intend a full-fledged assault on the desktop metaphor but rather seeks to give users—particularly high-end businesses willing to pay premium prices—a choice in how their employees see and manipulate information on a computer monitor. The company's flagship technology is Star Tree, first developed at PARC in 1993. In the 1980s Xerox missed out on profiting from the desktop metaphor it developed; Inxight was founded in part to avoid that mistake with Star Tree, an alternative that uses space, rather than time, as an organizing principle.

Star Tree replaces hierarchies of pull-down menus with on-screen icons, whose relationships to one another can be viewed at a glance. A Star Tree-generated map of a Web site, for example, might show an icon representing the page you are currently on, with lines radiating outward to icons representing links from that page. You can also see what is linked to the links and so on—four layers of relationships at any one time, arranged on your screen in the shape of a globe *(see Star Tree screen shot, left)*. If you want to find a particular set of links, you can spin the globe around on any axis by simply moving your cursor around the screen. It's a visually appealing way to organize information—like Web pages or organizational charts—and it allows you to see relationships among files more readily than pull-down menus do. But Rao admits that the obstacles to getting the concept adopted widely are huge, and that his primary goal isn't to overthrow the desktop metaphor but to become a part of it. "So when Microsoft says, 'Hey, we want to make this a part of Windows, so sell it or we're going to pulverize you,' then boy, we've won," he says. "That is the goal. I'd love to hear that."

Metaphor Trouble

Even Microsoft apparently sees the limitations in the desktop metaphor. The software Goliath has tried to introduce new metaphors on a regular basis—even though it has the most to lose if there is

ever a disruption in the status quo. When the changes have been too literal or too radical, they have failed, even with the clout of Microsoft's marketing behind them. For instance, Microsoft Bob, introduced in 1995, used the metaphor of a cozy-looking living room, complete with an animated guide, to help users navigate their computer systems. It was designed with new computer users in mind, as a way to give them a sense that they had nothing to fear. It failed spectacularly, mostly because the metaphor was so literal that it got in the way—users spent too much time navigating the desktop, trying to figure out how the virtual furniture, shelves and cozy fireplace related to a task like opening a file or application.

With Bob, in other words, it proved impossible to ignore all the distracting elements of the virtual living room. "In one sense the notion of 'metaphor' can get you into trouble," says Rao. "We call it the 'desktop metaphor,' but the metaphor isn't really very completely drawn out. It was just something to call it in the beginning, and after a while the computer desktop metaphor became its own thing, rather than something we thought of as like something else. There have been times people try to extend the metaphor, to make it look more like a desk or let you have piles of stuff like a real desktop, and it never works."

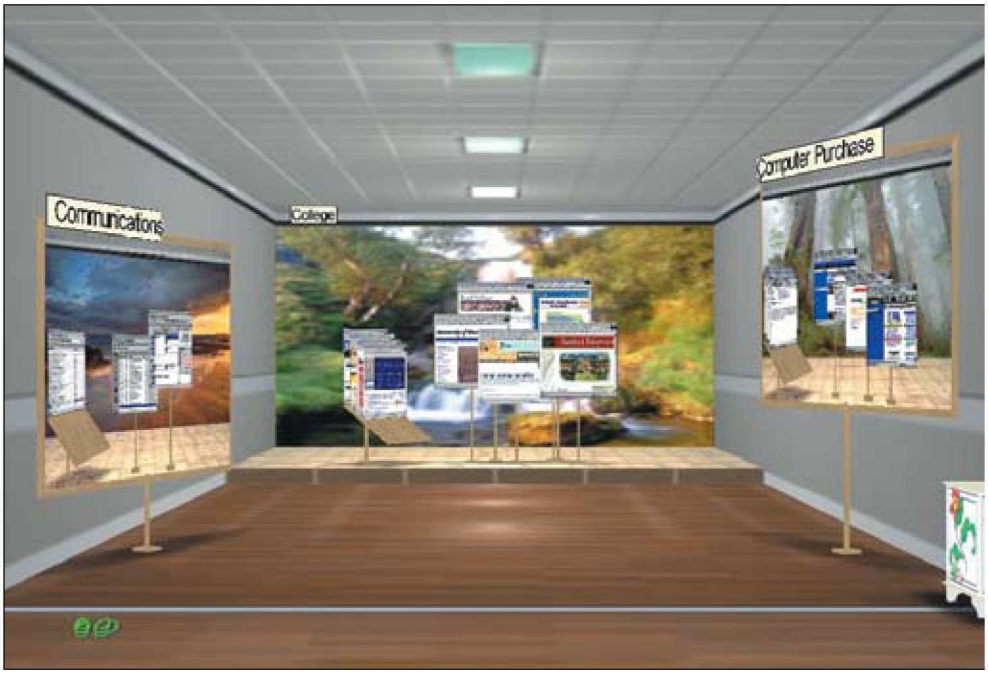
Through Bob's failure, though, Microsoft claims to have learned some things about what will work in new on-screen metaphors. For instance, Bob's idea of an animated guide lives on in current versions of Windows as Clippy. While this personified paper clip is still far too obtrusive for many people—the little assistant is turned off by default in the new software—Microsoft researchers maintain that the idea behind it is extremely compelling. That's because it points the way toward a design, alternatively known as an "adaptive" or "attentive" or "intelligent" interface, where the computer senses what we need and gives it to us. Call it the "friendly mentor" metaphor.

"We're interested in an interface that adapts based on what the user is trying to accomplish," says George Robertson, senior researcher with Microsoft's user interface research group and formerly a principal scientist at Xerox PARC. "We try to build models of what the user is doing, but also to understand the nature of interruptions." He notes that part of the problem now is that "Clippy tends to interrupt you when you're in the middle of typing." For instance, every time you type in the date in a Word file, it asks you if you need help formatting a letter. Microsoft is working toward solving that problem by building an inference engine that can anticipate your needs based on what you're typing, as Clippy does, but won't interrupt you. Rather, like a helpful personal servant, it will keep its observations to itself until you ask for help.

Conceivably, an inference engine can be made so intelligent that any change in the desktop metaphor itself becomes unnecessary: machines would automatically present information to you as you need it, eliminating the clutter and confusion that currently plague our computer desktops. If developers were able to build that degree of intelligence into our computers, they'd no longer need to overcome the high hurdle of educating all of us about how to use a new metaphor. Instead, we'd use the old one, but with far better results—much the way we use the same "interface" to drive automobiles today as in the days of the Model T. But behind that relatively unchanging interface, new tools such as antilock brakes, power steering, fuel injection systems and computerized warning systems aid us tremendously as we drive.

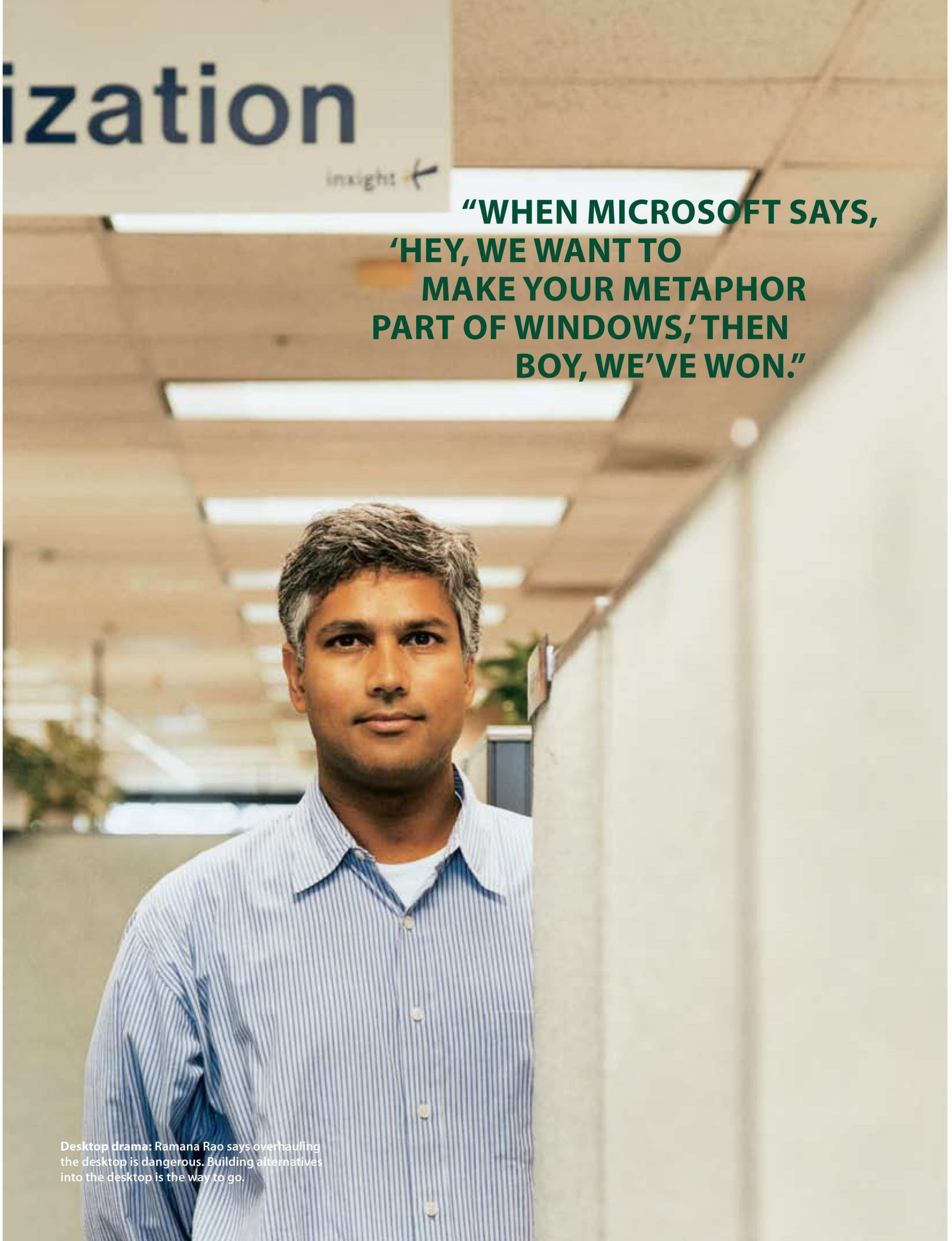
But that may be getting ahead of things. A nearer-term solution to the data glut and file loss perpetuated by the desktop metaphor will be to use 3-D graphics techniques, currently in vogue only in games and science and engineering software. "From our experience [with user groups], 3-D can make a real improvement," Microsoft's Robertson says. "It's possible to pack a lot more information into the same screen space. You're taking advantage of human perception and our ability to see depth relationships. You're also taking advantage of human spatial memory. In the real world, if I put a piece of paper in a pile, I can remember where it is weeks later."

One of Microsoft's long-standing research projects to employ 3-D space is Data Mountain, which allows you to place files on what looks like a surface tilted at a 30-degree angle so that objects at the top of the screen appear smaller and farther away. Robertson found that spatial memory allowed participants in user studies to remember exactly where they had stored up to 800 images on the "mountain," even after an absence of six months. "It works very well for storing things like photos or favorite Web sites because these things look different, and



COURTESY OF MICROSOFT

Wall mart: In Microsoft's new on-screen interface called Task Gallery, 3-D graphics help users remember where they placed their files, e-mail or Web pages. Users can walk through the virtual gallery's different rooms and store their files simply by "hanging" them on the walls.



"WHEN MICROSOFT SAYS, 'HEY, WE WANT TO MAKE YOUR METAPHOR PART OF WINDOWS,' THEN BOY, WE'VE WON."

Desktop drama: Ramana Rao says overhauling the desktop is dangerous. Building alternatives into the desktop is the way to go.

it's very easy to spot the differences even when the images are small," says Robertson. He concedes that Data Mountain works less well for documents; while thumbnail-sized images of pictures can be easily recognized, documents shrunk to that size all look more or less the same, making it very difficult to distinguish one from the other.

Another current research project at Microsoft that employs the virtues of 3-D is Task Gallery, where the metaphor is one of multiple rooms in which documents are "hung" until they are needed *(see Task Gallery screen shot, p. 57)*. By simply moving your mouse around the screen, you can "walk" from room to room in this virtual gallery, and hang the walls with miniature representations of your Word documents, Web pages, Adobe Acrobat files and so on. Conceivably, infinite "rooms" can be added, in which related documents and other files can be stored. However, Robertson admits that the project team has once again confronted the problem of people taking metaphors too literally. In user tests, for instance, participants balked at storing documents on the gallery's virtual "floors" or "ceilings," in effect reducing the usable space. Still, Robertson expects both Task Gallery and Data Mountain to become alternatives for organizing data in some Microsoft applications, most likely Explorer, in the next two years.

Layers of Paint

Visit any major company or university computer science lab around the world and you will likely find some kind of new interface work under way. Xerox PARC, the University of California, Berkeley, and Yale University, among others, continue to explore new on-screen metaphors. So does IBM, another powerhouse that, like Microsoft, is contemplating the demise of the desktop and sees "attentive" computing as an inevitable development. Its BlueEyes project uses a combination of sensors, video cameras and microphones to interpret your facial expressions, where you're looking and even what you're saying. That way, rather than clicking your desktop Web browser, you can access Internet information through very subtle human-computer interactions. You could verbally ask your Web browser to go to CNN Online. While you're there, the browser might observe where you look on the page and offer pages with related content for viewing—in theory making it virtually effortless to get what you want from your computer at all times without having to stop at the desktop.

"I have no doubt that in ten years our computers will be attentive in some appropriate way," says Robert Morris, director of the IBM Almaden Research Center. "As we learn more about human behavior, and what is considered okay and not okay from a privacy perspective, we will learn, and we'll eventually end up with a great interface."

But at least for the foreseeable future, interface designers see such work as an alternative to, rather than a replacement for, the desktop metaphor—a view shared by even the most caustic critics of the desktop. "Software today grows in layers, where we put the new over the old, like slapping a new coat of paint on," says Gelernter. "When people instituted browsers they didn't throw out Windows, and when they instituted Windows they didn't throw out DOS." By layering these alternatives over Windows, designers can drastically reduce the learning curve and hasten acceptance of their innovations.

However, some researchers in the field of human-computer interaction think it's time to throw out thinking about "metaphor" altogether—after all, it hasn't gotten us too far since the 1970s—and to begin designing devices that have no metaphor, no real-world analogy. It's not the desktop metaphor that's holding us back, they say; it's the whole notion that we need to make computers act like something other than what they are.

"I've spent too much time with metaphors," grumbles Don Norman. "The main problem with the metaphor is that it's just a stand-in for something else. It's not the thing you're using. It may help a beginner user for the first 15 minutes, but after that it gets in the way. When I drive I don't need metaphors. I turn the steering wheel left, and I go left."

It's not just the desktop metaphor that needs fixing, in other words, but the whole PC package, the way we relate to our computing devices. The desktop metaphor is so tightly wedded in our minds to keyboard, mouse and monitor that unless the outside package changes, the on-screen presentation doesn't have much of a chance to evolve either. Break out of that design, though, and all sorts of things become possible.

Alias/Wavefront's Bill Buxton predicts a world where the personal computer stops trying to be a general-purpose device, like a Swiss Army knife, and goes back instead to what it is good at: making text documents and spreadsheets. The problem isn't the desktop metaphor at all—it's that we're trying to use our personal computers for tasks they weren't meant to perform. Peel those tasks away to specialized devices—music to MP3 players, films to movie players, news and information to specialized readers—and you've solved the desktop metaphor problem. Each device will evolve its own best interface, depending on its specialized use. Buxton's favorite evidence of this process is the Palm Pilot.

"The heart of Silicon Valley was littered with the corpses of companies trying pen-based computing," he says. "You had Eo, Go, Momenta, Grid…then along came Palm. It did nothing that couldn't have been done before but did it right. So even though we'll have many apparent failures of new design concepts, there will be companies that go back and get it right."

Throwing out the desktop metaphor, however, might be even tougher than replacing it with new metaphors—and not everyone agrees that the PC is on its way out. "That kind of thinking is wrong," says Gelernter. "The PC isn't a Swiss Army knife. It's like a hammer. People don't want a million different tools. They want a single hammer that can do a million things, because it's a tremendously flexible, elegant and powerful tool."

But even if the desktop metaphor never goes away completely, it will likely recede, buried perhaps beneath Robertson's Data Mountain or Gelernter's Scopeware. Or maybe, as Buxton predicts, it will drift back into performing only the tasks for which it was created and for which it is uniquely suited. What flowering of alternatives will replace it is still a matter of some conjecture. But if the tenacity of researchers in the field is any indication, big things are bound to happen eventually. As cyberpunk author William Gibson has said, the future is already here. It's merely a question of figuring out which future it's going to be. TR

Join an online discussion of this article at www.technologyreview.com/forums/info

ARCHIBALD

THE INNOVATORS

HOW TECHNOLOGY IS TRANSFORMING EXISTING INDUSTRIES AND CREATING NEW ONES

TR100 THE YOUNG INNOVATORS WHO ARE CREATING THE FUTURE

Technology Review's Biennial TR100

Technology Review, the authoritative source on innovation, is proud to bring you the TR100—a unique biennial gathering of today's top young (under 35) innovators and key leaders in technology and business.

The outstanding work of the TR100 has a profound effect on the world today. Their innovations launch new businesses and create new industries. Air traffic control, oil exploration, electric power, automated stock trading, advanced medical diagnostics, bio-engineered drugs, wireless communications, broadband Internet, nanotechnology, robotics, computer crime investigation and hazardous-waste disposal are just a few of the areas influenced by the TR100.

The event acknowledges and celebrates the men and women who work in our most important and dynamic industries. An elite panel of judges, including two Nobel laureates and a host of leaders in business and academe, helps the editors of *Technology Review* identify 100 top young innovators who are creating the future. Through

Simplicity and fraud prevention are helping PayPal make digital payments real. A worried credit card industry takes note. Photographs by Misha Gravenor

BY EVAN I. SCHWARTZ

DIGITAL CASH PAYOFF

Around the time he immigrated to Chicago from Ukraine as a teenager in 1991, Max Levchin became obsessed with cryptography. Living under the old Soviet regime convinced him of the need to carry out communications undetectable by authorities. As a computer science student at the University of Illinois, he immersed himself in the mathematics of creating and breaking codes, not only making it the focus of his studies but also, he says, turning his pursuit into a "huge hobby" that consumed countless days and nights at the supercomputer center on the Urbana-Champaign campus. Dreaming that he would one day profit from his passion, Levchin aimed to start a company that would process financial transactions over the Internet, devising codes so secure that hackers wouldn't be able to read the data even if they intercepted them. He moved to Silicon Valley after graduation in 1998 to make good on his goal.

Fraud fighter: Max Levchin's fraud detection software helped make PayPal the first successful digital-cash company.

It didn't quite go as planned—but close. Now a worldly 26 years old, Levchin is the cofounder and chief technology officer of PayPal, the Palo Alto, CA, company that has suddenly become the leading processor of person-to-person, or P2P, payments over the Internet. Just as Napster allowed people to directly share music online, PayPal enables people to exchange money instantly without having to open expensive merchant accounts to accept credit cards. Yet to Levchin's surprise, advanced cryptography has had little to do with PayPal's success. Rather, the company's rapid adoption by millions of small businesses and individuals operating chiefly on Internet auction site eBay is largely credited to Levchin's more recent obsession: developing financial surveillance software that closely monitors PayPal's customers and almost instantly alerts both the company and law enforcement officials to any suspicious account activity. “We mine millions and millions of transactions in real time,” Levchin says.

AT A TIME WHEN FEW STARTUPS CAN EXHIBIT A CLEAR COMPETITIVE EDGE, PAY-PAL'S FRAUD-MONITORING SOFTWARE MAY BE A TECHNOLOGICAL SILVER BULLET.

Limiting illegal transactions is crucial to the long-term survival of Internet commerce. Since consumers aren't typically liable for fraudulent use of their credit card numbers, they usually don't worry much about these numbers, or even their very identities, being stolen. Merchants, however, are keenly interested in stopping such swindles, because they are the ones who have to eat what is estimated to be $2 billion in annual credit card fraud losses, with a disproportionate share of those losses occurring online. Whereas Visa reports an overall fraud rate of .07 percent, a Gartner study of Web merchants indicates the figure soars to 1.13 percent for online transactions. In other words, buyers and sellers online face a 16 times greater risk of not being able to recover the money or merchandise due to them.

PayPal claims it has found a way to bring the online fraud rate down to less than .5 percent, thus eliminating 60 percent of the risk of taking credit cards online. It is this ability to combat criminal behavior that has enabled the privately held company to raise a whopping $211 million in equity financing, with more than 40 percent of that coming *after* the great Internet implosion that abruptly ended so many getrichquick.com schemes. And in September, PayPal announced plans to complete an IPO worth up to $80.5 million.

At a time when few startups can exhibit a clear competitive edge, Levchin's fraud-monitoring software—dubbed Igor, after a Russian hacker it helped detect—may very well be a technological silver bullet that largely eliminates one of the chief obstacles to conducting commerce with strangers around the planet. But PayPal's potential for widespread growth has been a cause for alarm in the $2.7 trillion credit card industry, which seems fearful that the company could displace Visa and MasterCard, first on the Internet and then offline. PayPal could “cut the legs off of banks and credit card companies,” says Kjell Hegstad, senior vice president of business development at ING Direct, a U.S. arm of Dutch banking giant ING Group, which has taken a “know-thy-enemy” approach to matters by investing in the upstart.

FRAUD SQUAD

The backbone of PayPal's success is its fraud squad. Levchin heads a team of 100 employees, about one-sixth of the company's personnel, who work full time fighting fraud and fine-tuning Igor's ability to ferret out scams. By watching Igor's constantly changing graphics for red flags, alerts and statistical anomalies, the fraud fighters can pinpoint accounts exhibiting unusual patterns of activity that signal certain transactions may be fraudulent—things like one user attempting several transactions at once, high dollar amount transfers, or payments being sent to notorious locations or unverified addresses. “The system is conducive to rapid investigations,” Levchin says. When Igor detects dubious activity, humans review the evidence and decide whether to freeze the corresponding accounts.

Igor has to not only move quickly but also be right. As it tested early versions of the software, PayPal was hit with a customer backlash when Igor got overzealous and prompted employees to inactivate many legitimate users, who were suddenly unable to send and receive money. When those users couldn't get through to PayPal's flooded customer service department, a spate of complaints to the San Jose, CA, Better Business Bureau followed, leading to a public-relations disaster. The company has since refined Igor to hone in on only the most suspicious behavior patterns, and it has staffed an Omaha, NE, call center with more than 400 customer service specialists and operations staff to handle inquiries and quickly unfreeze accounts when appropriate.

PayPal also has several patent-pending techniques for verifying its customers' identities. For example, when a member signs up to allow the company to directly debit and credit her checking account for PayPal transactions, the company makes two tiny deposits into that account—say 14 cents and eight cents. Once the member learns the amounts (from an online, phone or paper bank statement), she must enter the correct figures on PayPal's Web site to activate the link. “This verifies their identity and tells us that this person has control over that account,” says Levchin.

Once the user's account is active, Igor's pattern detection algorithms start monitoring it. While Levchin won't reveal much about what Igor looks for, this much is clear: Igor incorporates some of the oldest and newest techniques from the field of artificial intelligence. It is an expert system that knows a series of rules (for example, if money is being transferred from a U.S. user to a foreign one, then check whether the foreign user is in a country approved for PayPal usage). Igor also incorporates a neural network that “learns” new types of fraud over time. If a certain user keeps linking new credit cards to his PayPal account, then opens another account under a different e-mail address and attempts to link some of the same cards, Igor will learn the intricacies of that scam and watch more carefully next time.

Policing electronic payment activities is becoming more and more challenging. Last May, officials from the Federal Bureau of Investigation revealed the results of Operation Cyber Loss, a sweep of stings that led to the arrests of 90 hackers charged with defrauding 56,000 citizens of $117 million, mainly through online auction fraud, stolen credit card numbers traded and used over the Internet, and wholesale identity theft. Months before those arrests, PayPal and the FBI first began sharing data and evidence with each other. Levchin says that FBI agents have been dropping by PayPal's offices on a regular basis, comparing Igor's red flags with tips that the FBI collects through its Internet Fraud Complaint Center Web site.

TROUBLE-FREE TRANSACTIONS

Both senders and receivers of cash have primarily been drawn to PayPal not for its safety but for its speed and simplicity, especially when it comes to completing messy eBay transactions. In the past, the seller of a vintage guitar, a rare book or any other eBay item had two ways to receive payments—either via a check sent through the mail or by accepting credit cards. Before PayPal arrived in October 1999, 90 percent of eBay transactions were completed by check, a process that typically takes five to 10 business days, as sellers generally wait for the check to arrive and clear before they ship their merchandise. Credit cards, although timely, are impractical and too expensive for part-time merchants and individual sellers, as account charges and transaction fees can consume upwards of six percent of each payment.

PayPal promised a way to solve this conundrum by making it possible to instantly complete transactions, a feat that prompted thousands of eBay sellers to begin offering it as a payment option. When the first million buyers responded to PayPal's offer of a $10 incentive (since cut to $5) just to sign up, the service quickly achieved critical mass.

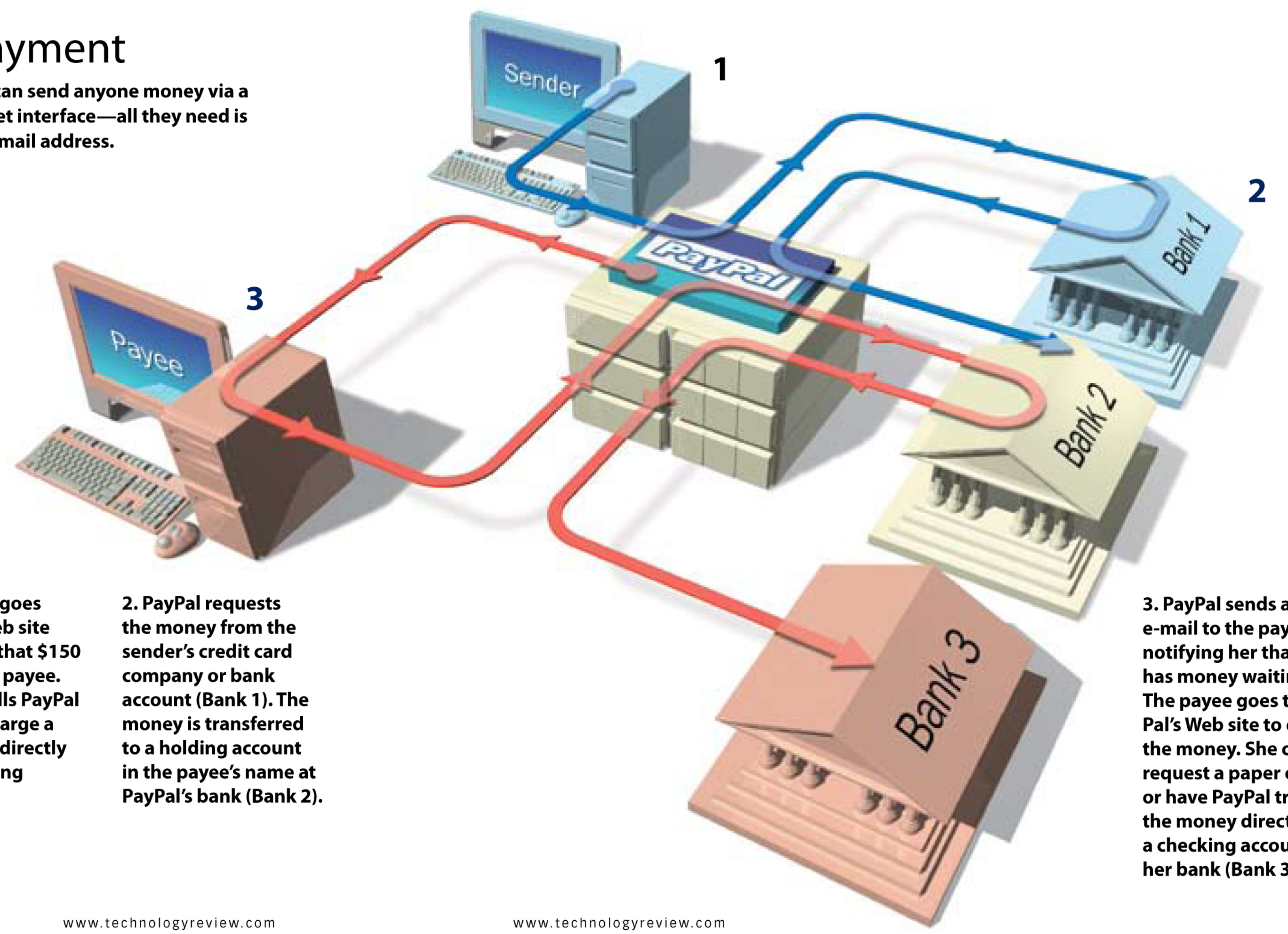
A user enrolls at the company's Web site by linking an existing credit card or checking account to a new PayPal account. A valid e-mail address for the recipient is all one needs to send someone else money; her name and physical location aren't required. The recipient receives a message letting her know that her money has arrived. If she is not already a PayPal member, she must sign up to claim her funds, which can be transferred to an existing checking account (or sent by check). PayPal's process has made sending money as instantaneous and convenient as e-mail itself. Since anyone can pay anyone else this way, PayPal's service has rapidly transcended eBay and is now accepted at more than 20,000 Web sites—and can even be used to pay debts incurred offline. If you owe a friend $6.50 for lunch, you can use PayPal to e-mail him the cash using any Internet-enabled device, from a cell phone to a palmtop gadget.

So far, the best proof of PayPal's success is its viral rate of growth, from virtually nothing two years ago to more than 200,000 transactions completed each day. That's still a far cry from Visa's aggregate volume of over 200,000 transactions every minute, and it represents less than five percent of all e-commerce. But PayPal, in short order, has become the most visited Web site for personal finance, and it processes payments

P2P Payment

PayPal users can send anyone money via a simple Internet interface—all they need is the payee's e-mail address.

SLIM FILMS



1. The sender goes to PayPal's Web site and requests that $150 be sent to the payee. The sender tells PayPal whether to charge a credit card or directly debit a checking account.

2. PayPal requests the money from the sender's credit card company or bank account (Bank 1). The money is transferred to a holding account in the payee's name at PayPal's bank (Bank 2).

3. PayPal sends an e-mail to the payee notifying her that she has money waiting. The payee goes to PayPal's Web site to claim the money. She can request a paper check or have PayPal transfer the money directly into a checking account at her bank (Bank 3).

for one out of every four eBay auctions.

Unlike many popular dot coms, PayPal is supported by a business model that Peter Thiel, PayPal's 34-year-old CEO, says will bring in nearly $100 million in revenue in 2001, making the company profitable. While PayPal was free for both buyers and sellers during its first year in business, sellers who accept credit card payments now must pay a 2.9 percent fee, plus a flat 30-cent-per-transaction surcharge, which adds about another half a percent to the tab for the average PayPal transaction of $50. Volume continued to explode even after PayPal imposed these fees. That's because traditional credit card companies charge online merchants even more—as much as six percent. Thiel claims that PayPal can turn a profit on such low transaction fees because of its success minimizing fraud.

ANXIOUS COMPETITION

All this growth hasn't gone unnoticed by the giants of the credit card industry, which have been scrambling to catch up. Bank One, one of the nation's five largest bank holding companies and parent of credit card company First USA, launched eMoneyMail in March 2000. Within six months, however, the online payment service shut down after experiencing a fraud rate reported to be as high as 25 percent. Bank One spokesperson Tom Kelly confirmed an unacceptably high fraud rate but said, "I don't think we have a lot of interest in talking about it."

In the fall of 2000, Citibank, the nation's largest bank and credit card issuer, introduced c2it (pronounced "see-to-it"), a P2P system being marketed via multimillion-dollar deals with Microsoft and America Online. It only managed to sign up 100,000 customers in its first year, despite offering a $10 sign-up bonus, but officials aren't letting up. "This business is strategically important to Citi," says Antony Jenkins, chief operating officer of c2it. "At the end of the day, processing transactions is what banks do."

Then there's eBay itself, which acquired PayPal rival Billpoint and began running it as a joint venture with San Francisco banking conglomerate Wells Fargo in March 2000. All these competitors combined have managed to eke out only a tiny market share against surging PayPal. "PayPal had a bit of a head start," says Kevin Pursglove, eBay's senior director of communications, "and they are very aggressive." He adds, however, that "the market is still young," and that eBay thinks Billpoint will soon begin to achieve something like PayPal's critical mass.

Traditional credit card issuers seem to be spooked by PayPal, and not just for fear of losing out on online transactions. To understand why, one must understand a basic fact about PayPal's business model. Let's say that Julia has just won an eBay auction for an antique lamp, agreeing to pay $276 plus $24 in shipping costs. The seller, whom she only knows through the eBay handle LampMan and his e-mail address, lampman@netmail.com, advertises that he accepts PayPal. Already a PayPal member, Julia goes to PayPal.com to send the $300 total payment to that e-mail address. At that point, she has two options. She can instruct PayPal to charge her Visa or MasterCard, or she can have the amount debited directly from her checking account.

Although PayPal claims to be indifferent to the outcome, Julia's choice makes a big difference financially. If she opts for the credit card, PayPal becomes the merchant of record on the transaction and must pay Julia's credit card company a two percent "interchange fee." After collecting the same two percent from LampMan, PayPal essentially breaks even. But if Julia chooses her checking account, PayPal doesn't have to pay the fee, and it still collects the two percent from LampMan. PayPal, therefore, has the financial incentive to shift as much business as possible to checking accounts. However, if PayPal moves too aggressively to phase out use of credit cards, it risks antagonizing Visa and MasterCard, which currently offer the company their lowest fees, under the assumption that PayPal is significantly increasing the industry's overall volume.

Thiel and Levchin are careful about such questions. "Yes, we make a bigger margin [on checking-account transactions]," Thiel says. "But we don't envision displacing Visa and MasterCard. We are enabling consumers to make their own choices. We can't force them."

PayPal's attempts to get customers to abandon traditional banks and credit cards belie this statement. One such enticement: the PayPal money market fund, managed by Barclay's Global Investors. Under this option, buyers and merchants can earn money on the funds they keep in their PayPal accounts, which makes transactions even simpler and more profitable for the company. More recently, PayPal introduced debit cards, so that customers can use their PayPal accounts for offline transactions as well. If PayPal's more than 10 million members start using the new debit card instead of credit or debit cards issued by MasterCard and Visa, these giants may begin to see their market share erode.

So Thiel's claims about having no designs on credit card companies aside, these moves, along with PayPal's recent launch of an online bill payment service, have exacerbated fears that the company has set its sights beyond online transactions. Such suspicions are rampant even among the company's own backers. PayPal's seed money has come not only from traditional venture firms like Goldman Sachs and J. P. Morgan Chase but also from banks like ING, Providian and Germany's Deutsche Bank, which are hedging their bets against PayPal's expansion. "Unless they're partnering with PayPal, banks aren't keen to see it succeed," says ING's Hegstad. "What bank would want to give up ownership of its customers?"

Citibank, with its c2it service, is especially anxious to counter PayPal before growth gets out of hand. "This is a huge opportunity," says Citibank's Jenkins. "Technology always changes the way financial services get delivered. Credit-scoring software and database marketing led [30 years ago] to the credit card industry itself. In the future, we think that everyone who now has a credit card will also have a P2P account." But in the wake of debacles like Bank One's eMoneyMail, Citibank is proceeding cautiously. "We wanted to understand the fraud component before we mass-market the product," adds Jenkins.

DETOURING HISTORY

Even as it contemplates past lessons, Citibank is following a strategy plotted by PayPal—which has already learned so well from past failures that rivals may find it difficult to catch up. Indeed, PayPal's founders are adamant they wouldn't have achieved their current position without learning from early failures in the digital-payments marketplace.

Sitting pretty: In a market littered with failures, CEO Peter Thiel's business strategy has made PayPal a P2P payments giant.

The company was born in the fall of 1998, when Levchin, newly arrived in California, attended a lecture at Stanford University given by Thiel, then running his own hedge fund. The two got to talking afterwards and made a breakfast appointment for the following morning. By the end of that meal, Thiel had agreed to help find funding to develop and market Levchin's software, which at the time scrambled transactions sent between mobile Internet devices.

As he took up the quest, however, Thiel immediately hit a solid stone wall of skepticism. Although funds were flowing freely to thousands of half-baked Web ploys at the time, the market the two men were eyeing was already littered with high-profile fiascos like CyberCash, DigiCash and First Virtual as well as dozens of lesser-known flops aimed at popularizing new brands of encrypted digital currency for online payments. "We met with a hundred different venture capitalists," Thiel recalls. "A lot of people told us it was insane to be going into this space."

As the company struggled to get off the ground, however, Levchin and Thiel delved deeply into the state of digital-cash technology in order to learn from the spate of calamities and bankruptcies in that market. "There are a half a dozen different theories about why DigiCash and all the others failed, and all the theories are valid," says Thiel. "We tried to avoid making the same mistakes."

The first mistake involved complexity. Most of the early digital-cash solutions required users to download hard-to-use software, known as digital wallets, that encoded money in an encrypted format; consumers simply refused to go to all that trouble just to pay for something. What's more, merchants had to adopt a standard called Secure Electronic Transactions for deciphering encrypted payment codes; those systems typically required the purchase and installation of sophisticated workstations.

PayPal opted for the far simpler Secure Sockets Layer encryption method—built into most browsers and already used by many e-commerce companies—to scramble data sent by its customers. The system also relieves merchants from the obligation to protect their customers' financial data; indeed, that data is never in their hands. PayPal sends no payments or payment codes by e-mail. Only notifications about transactions are transmitted over the Internet. When money is transferred between accounts, the debits and credits happen only on PayPal's secure servers in California, which cannot be accessed over the Internet. "All the money lives and dies on our servers," says Thiel. "We decided to force all the complexity of keeping transactions secure upon ourselves," adds Levchin. "Consumers and merchants shouldn't have that burden."

PAYPAL HAS SUCH A HEAD START THAT RIVALS MAY FIND IT DIFFICULT TO CATCH UP.

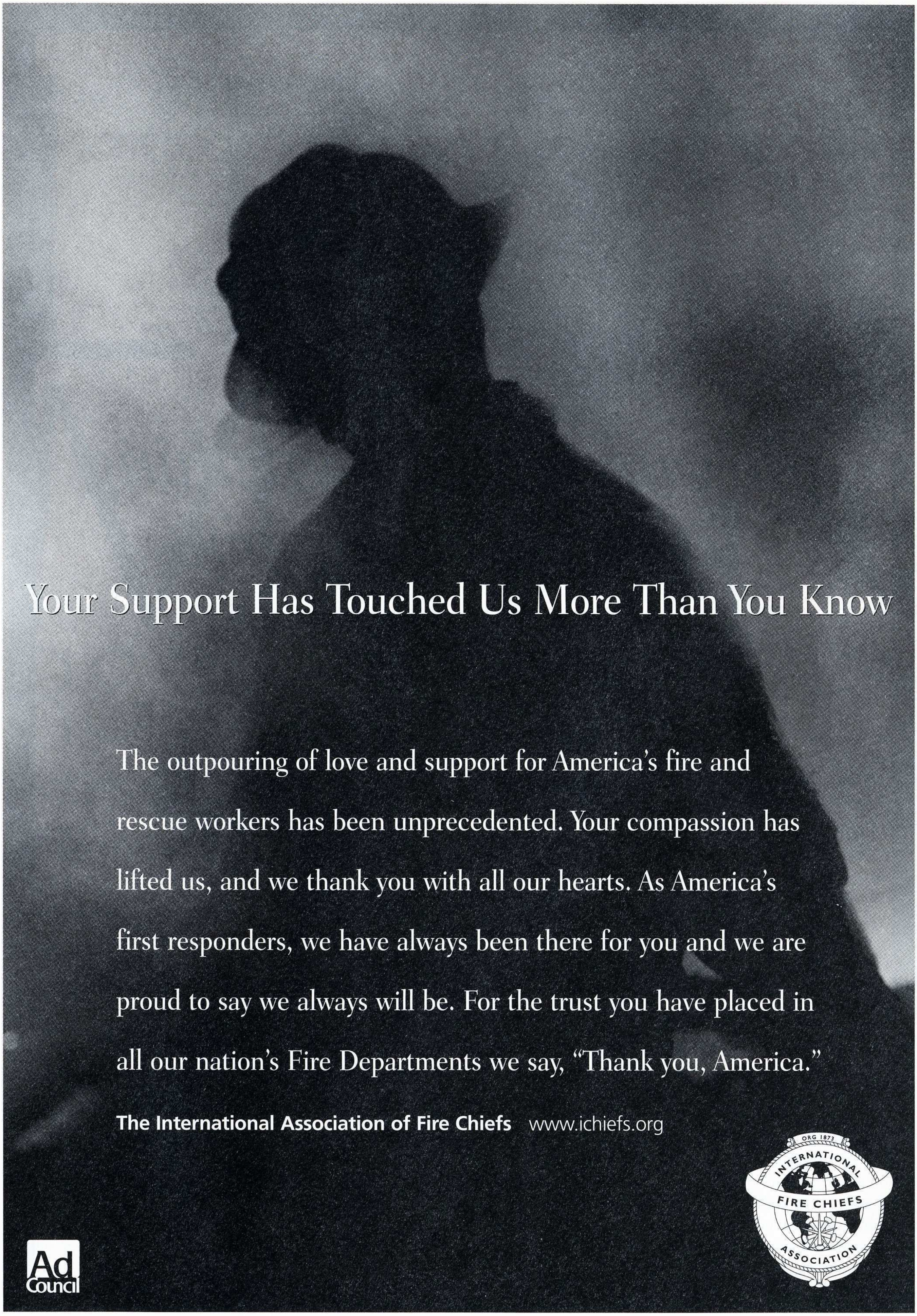
Micropayments were another holy grail of some early digital-cash companies. Ill-fated ventures like First Virtual and Digital Equipment's MilliCent aimed to create payment systems that could handle transactions under $5—even those of just a few pennies—potentially opening up vast new markets for selling news articles, songs and other low-priced information goods. Yet micropayments never caught on, possibly because users didn't appreciate being nickel-and-dimed to death and possibly because there really isn't much money to be made collecting change. "It reminds me of that *Saturday Night Live* skit," Thiel says, about the First Citiwide Change Bank, which specialized in exchanging coins for dollar bills. The punch line was, "All the time our customers ask us, How do we make money doing this? The answer is simple: volume."

Instead of promoting micropayments as a separate market, PayPal simply processes small charges like any other transaction. While the maximum is set at $10,000, PayPal will process payments as low as one cent. The company, of course, loses money on such tiny transactions, but Thiel says there haven't been enough of those to cause a problem. "If it becomes a major expense," he says, "we could change our policy very quickly."

Another roadblock for early digital currencies was their lack of liquidity. DigiCash and more recent flops, like Flooz (a currency used for giving gift certificates that could be redeemed at certain Web sites), weren't denominated in dollars but were more like poker chips in a casino. You couldn't spend these strange new digital currencies universally, and that made people reluctant to accept them. "Money needs to be liquid," says Thiel. "The most popular currency in the world is U.S. dollars." PayPal has customers in 36 countries, and it charges higher rates for international money transfers. But to keep transactions on one simple level among all its members, there are no currency conversions. With PayPal, everything happens in U.S. dollars.

By far the biggest obstacle for any company trying to create a universal payment system is trust. Visa, MasterCard, American Express and Discover have spent billions of dollars building up trusted brands through advertising and marketing campaigns. PayPal has hardly spent anything. Instead, it issued a guarantee. It now ensures merchants that follow certain rules that it will reimburse them for any fraudulent transactions. The chief rule is that merchants must ship all merchandise to the account holder's official address, with no items going to a buyer's "office address," for instance. Stealing a credit card number, insisting on a phony shipping address, walking away with the goods and sticking the merchant with the bill is one of the most popular swindles on the Internet. PayPal's rule and guarantee may seem simple (though the company has drawn some heat for not extending the same protection to defrauded buyers), but mainstream credit card companies have been unwilling to take even those steps.

Fighting financial fraud in a world of interconnected data networks isn't just a way to save some money; it is and must remain one of the core competencies of the world's banking system. That's why, possibly fearing PayPal really has developed technologies and tactics to combat con artists better than anyone else, especially in the tricky Internet commerce arena, the giants of the industry have organized themselves to fight back. In recent months, longtime rivals Citibank, Bank One and Wells Fargo banded together with some two dozen other companies to form Project Action, an alliance aimed at standardizing secure Internet payment transactions. In what could be the ultimate compliment, PayPal hasn't been recruited to join. TR


Your Support Has Touched Us More Than You Know
The outpouring of love and support for America's fire and rescue workers has been unprecedented. Your compassion has lifted us, and we thank you with all our hearts. As America's first responders, we have always been there for you and we are proud to say we always will be. For the trust you have placed in all our nation's Fire Departments we say, "Thank you, America."
The International Association of Fire Chiefs www.ichiefs.org
ORG 1873
INTERNATIONAL
FIRE CHIEFS
ASSOCIATION
Ad Council


Pick up a little something
for your chest pain.
Pick it up and dial 9-1-1 at the first warning sign of heart attack or stroke.
The faster you get help, the better your chances of survival and complete recovery. To learn more, visit our web site at www.americanheart.org or call us at 1-800-AHA-USA1.
American Heart Association®
Fighting Heart Disease and Stroke
This space provided as a public service. © 1999, American Heart Association

LEAN MEAN R&D MACHINES

Firms step outside their traditional roles to enhance the bottom line. BY WADE ROUSH

SCORE CARD

The pharmaceutical industry has a drug problem: it can't find enough new ones. Companies are under pressure to invent the next Prozac or Viagra, but without more efficient and cost-effective ways to develop new drugs, those kinds of blockbuster medications will remain once-in-a-decade discoveries. "It costs too much, it takes too long and it produces too little," says Rod MacKenzie, a vice president in Pfizer's Global Research and Development division, of the industry's traditional method of drug discovery. "The problem is, how do you change the engine while the vehicle is still moving?"

One solution to the problem of retooling Pfizer's $4.4 billion R&D engine is its Discovery Technology Center, a gleaming two-and-a-half-year-old facility in Cambridge, MA, where the company's scientists team up with academic researchers and small biotech firms to develop computerized methods for screening thousands of potential drug molecules per day. Key to the lab's strategy are its small size (just 70 researchers out of the 3,000 involved in drug discovery across Pfizer) and its location, at the center of the Boston-area biotech hothouse and a healthy distance from Pfizer's main R&D facility in New London, CT. "We're small and we're offline in the sense that we don't have the same day-to-day pressures of productivity that the other sites do," says MacKenzie, who directs the center. "And what happens here in Cambridge is that people beat a path to our door," including researchers from some of the area's top academic institutions.

The pharmaceuticals industry is hardly the only sector where researchers are under increasing pressure to find new ways of zeroing in on high-growth products and technologies. MacKenzie's critique of conventional research methods in the drug industry could be applied equally well to the chemical, aerospace, transportation, telecommunications and information technology sectors. And in each of these sectors, leading companies are looking for new ways to make their research groups nimble enough to react to ever changing technologies—and market opportunities.

For many, that means getting their researchers more connected—with each other, with their firms' customers and, as at the Discovery Technology Center, with their peers in academia. It can also mean looking more closely than ever before at their portfolios of research projects, personnel and capabilities, and loading this information into so-called knowledge management databases that guide decisions about which potential products

"The cost of doing R&D keeps going up, so you have to

and technologies to pursue. These approaches and other new strategies are gaining urgency as growing economic uncertainty—coming after years of good times and loose wallets—reminds chief technology officers of the need to prove the value of their companies' R&D spending.

Technology Review's second annual Corporate Research and Development Scorecard *(p. 75)* shows respectable increases in R&D spending in the 2001 fiscal year at the majority of companies. But the scorecard does hint at stormy financial days ahead. Spending is flat or declining at some of the United States' most notable technology firms, including Exxon Mobil and computer and telecommunications giants such as Compaq Computer, Silicon Graphics, Computer Associates, 3Com, Qualcomm and AT&T. And while most firms' R&D spending has remained steady this year when measured as a percentage of revenues, forecasts for plummeting revenues as the economy heads into a recession are likely to translate into less money for research next year. "We have seen over the last several years a tremendous increase in the rate of growth of industry R&D spending, but you can't sustain that rate of growth economically," says Jules Duga of Battelle, a nonprofit research institute in Columbus, OH. What's more, he says, "The cost of doing R&D keeps going up, so you have to spend more and more to gain less."

What the scorecard data don't show is the growing collection of industry R&D collaborations and new management approaches designed to counter just these challenges. Technology companies, in essence, are looking for ways to get a bigger bang for their R&D buck.

MAKING CONNECTIONS

In the pharmaceuticals industry, where R&D costs have been rising for years without any commensurate rise in the number of new drugs reaching the market, it's long been clear that old research models needed revision, says MacKenzie. Implementing a discovery process that produces more drugs over less time requires freeing researchers from the "pressures of productivity" that can keep them from experimenting with risky new technologies. At the same time, even a state-of-the-art research center needs to keep its work aligned with business needs. To that end, Pfizer's Discovery Technology Center hires only researchers who "have scientific degrees but are also outstanding data miners or statisticians on the side," says MacKenzie. Such people tend to be "totally immersed in the business of drug discovery, not off to one side of it, which is incredibly important to what we do."

To guarantee a supply of such researchers, Pfizer cultivates close ties with the local academic community. Last year, for example, the company created a three-year fellowship program in computational biology at Cambridge's Whitehead Institute for Biomedical Research. Fellows are expected to work inside the center for part of that time, examining gene sequences or protein structures relevant to drug discovery, but are also encouraged to do independent research. And for more great ideas, the center isn't opposed to turning to smaller companies and technology suppliers. Cambridge, MA-based BioTrove, whose nanoscale liquid-handling technology allows researchers to mix tiny quantities of reagents with 10,000 or more separate drug targets on a single chip, is conveniently headquartered right inside the Pfizer center's facility.

One of the basic tenets of the Pfizer center is that research is more effective—and more profitable—if it's more connected to the world outside the company. And Pfizer is hardly the only high-tech company testing this hypothesis. Chip-making giant Intel, for example, is spending part of its $4 billion R&D budget this year to support a series of "lablets" adjacent to top universities, each directed by a faculty member who has taken a leave of absence for a year or more. Each of the 20- to 30-person lablets will focus on a promising young technology *(see "Intel Revamps R&D,"* TR *October 2001)*. For example, computer scientist David Culler, the founding director of an Intel lablet at the University of California, Berkeley, is developing the software infrastructure for networks of tiny sensing and communication devices. If such devices eventually permeate our surroundings—gathering and wirelessly sharing information that could be used in surveillance, environmental control or scientific measurement—Intel wants to be the firm that builds them.

Key to this program, says Intel's director of research David Tennenhouse, is the fact that the academic researchers heading the lablets have a strong desire to see their ideas applied in the real world. Intel, however, is discouraging the researchers from taking their technologies all the way to the commercialization stage or becoming business unit managers, which might keep them from doing what they do best—innovate. "We're saying, 'Work on this strategic research project for a few years, and if it succeeds keep moving downstream [toward the market] for a few years, but then cycle back to the lab until you have another idea that you want to foist on the world,'" says Tennenhouse.

FOOT IN THE DOOR

If Intel and Pfizer are dismantling the old walls between corporate and university research, IBM is blurring another traditional boundary—that between corporate research labs and the company's own customers. The idea behind Big Blue's new Emerging Business Group is to offer small startup firms access to IBM's extensive research in information technology. In return, IBM may get a small amount of cash or equity, but the main point is to encourage the smaller firms to build their own new technologies on top of IBM software and services. "Basically, we get IBM platforms into those companies so that when they succeed, we have a growth market for our products," explains Dave McQueeney, IBM's vice president of emerging business. "If we pick the startup companies that will grow up to dominate new spaces, it could be very smart for us."

As an example, McQueeney points to work on online auctions at IBM's Thomas J. Watson Research Center in Yorktown Heights, NY. A team there is developing "combinatorial optimization" software that compares bids in Internet-based auctions where the bidders seek to buy distinct but overlapping sets of items. One bidder—say, an electronics manufacturer—may need components

spend more and more to gain less."

PIERRE-YVES GOAVEC

A, B and C to build a CD player, while another may need B, C and D to build a VCR. The software solves the surprisingly complex problem of knowing who, from the seller's point of view, has placed the most lucrative bid.

IBM could commercialize the auction software on its own, but it might actually be wiser to hand the technology over to a startup. "Say you are an auction company," explains McQueeney. "We say to you, here is this capability that we've had five PhD mathematicians working on for three years. We'll make it available to you now, but it's useless to you unless you run it on our infrastructure," meaning IBM's software and servers. Not only does the auction company get a big bang out of being first to market with the new software, but once other companies start adopting the technology, IBM gets to sell more infrastructure software. Just as important, IBM researchers are involved throughout the process, meaning they stay plugged into the latest trends and opportunities in their customer communities.

CUTTING THE FAT

The profusion of new, more fluid corporate research models can create a new problem: monitoring the results. If managers don't have a good real-time picture of what their researchers are up to, it's easy to wind up wasting money on redundant studies, underfunding promising technologies or letting moribund projects linger too long. But lately companies such as 3M have been getting serious about knowledge management, the use of searchable databases or intranets to archive what individuals and groups in an organization know and describe what they can do. Not only can that information foster creativity and new collaborations, it can also help chief technology officers decide whether to increase spending in areas of research viable in the current market or cut the fat where it's unlikely the company would be able to compete well.

3M managers companywide have strapped on their seat belts for a comprehensive spending review of R&D efforts instigated by new CEO W. James McNerney, who started last January. The first step was to build a database showing "where all of our [R&D] money was going in great detail, which was not something 3M had done before," says Steve Webster, vice president for research and development in 3M's corporate technology and transportation division. The database allowed "some very specific discussions about which opportunities are likely to have the biggest payoff, some that may not be so interesting and some that no one may be working on but which actually may be better opportunities than what other parts of the company are working on," says Webster.

As one result, 3M has decided to put even more money into building new electronic displays based on organic light-emitting diodes, already identified as a potential successor to the company's liquid-crystal display technology. The company also discovered it had underestimated its expertise in an important area: software design. In developing its knowledge database, the company surveyed each business unit about the R&D programs it depended upon. One of the technologies mentioned again and again in the survey belonged to a category called "Other." "We had to open the box and ask, what is it about 'Other' that provides so much growth?" recounts Webster. "In this case it was software and electronics," such as the technologies 3M sells to libraries to catalogue and track their books and deter theft. In fact, so many of 3M's products now depend on computers and software that the company realized it needed to shore up research spending on information technology. "When you think of 3M you think of films and coatings, but our systems integration is actually very important," Webster says. "Now we can quantify that"—and allot R&D resources accordingly.

Balancing an increased market focus—and closer ties to customers—with the pursuit of world-class science is now the trick for many corporate R&D groups. Gone forever are the days when large industrial labs churned out scientific papers and conducted long-term research far removed from business pressures. But while R&D groups have clearly gotten more business friendly over the last decade, they are also feeling pressures to come up with tomorrow's high-growth opportunities.

Indeed, industrial-R&D expert Richard Rosenbloom, an emeritus professor at Harvard Business School, is convinced that most high-tech firms—especially in the information technology sector—"still aren't doing enough to invest in the future technologies that will be the next big revolutionary business. They've been experimenting with new venture units, spinoffs, joint ventures and the like, but I don't know of a single big corporation that has a track record that is exceptional in any of those initiatives."

But if innovative efforts at doing research, like those being implemented at Pfizer, Intel and 3M, do ultimately help their companies pull ahead of the pack—and do so cost-effectively—other corporate R&D teams may soon be looking to turbocharge their own technology engines. TR


energy & power • industry & automation • information & communication • medical systems & healthcare • financing • lighting • transportation
SIEMENS
Global network of innovation
© Siemens Corporation, 2001

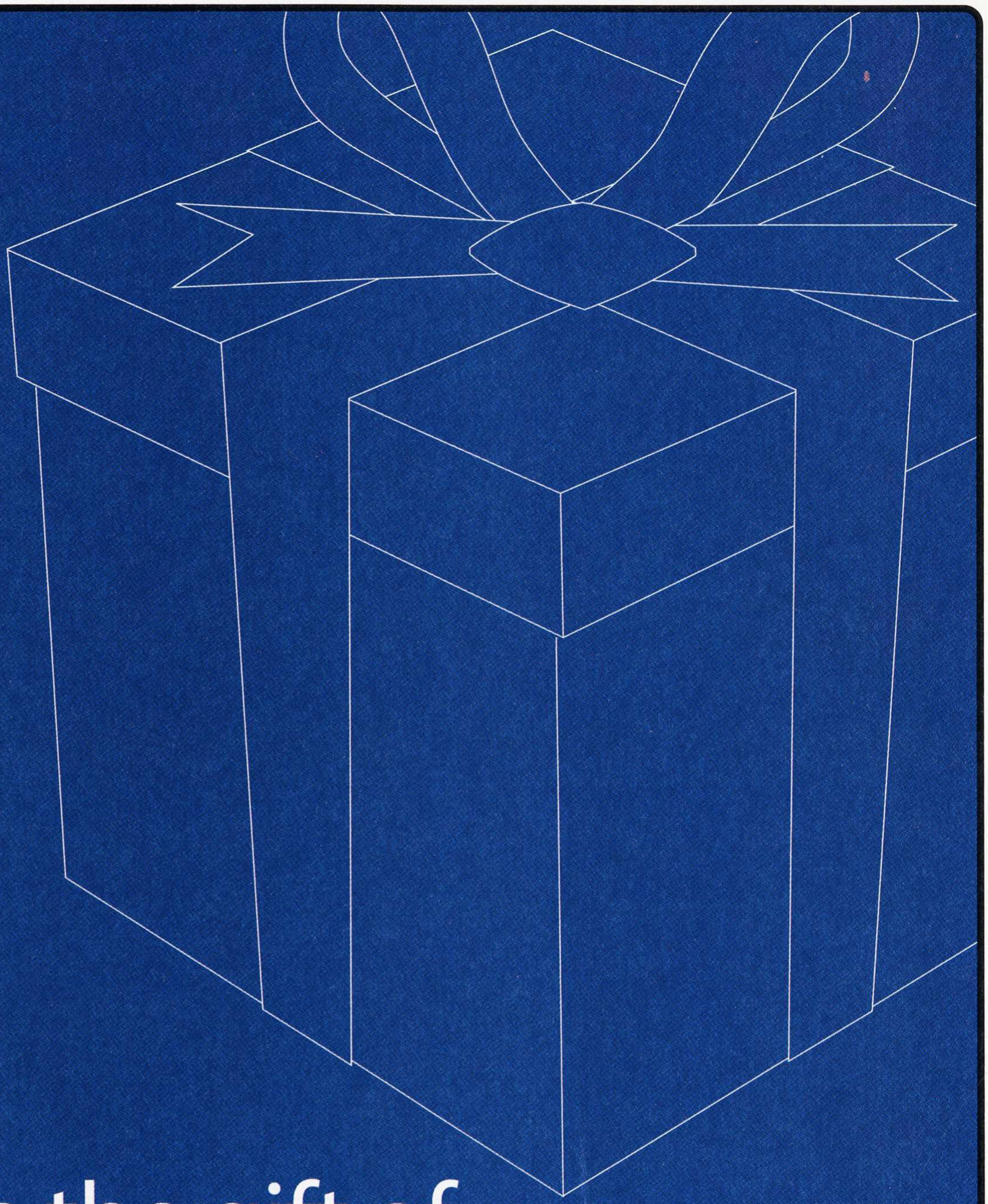
THE CORPORATE R&D SCORECARD 2001

The figures in *Technology Review's* 2001 R&D scorecard, derived from annual reports and U.S. Securities and Exchange Commission filings, cover fiscal years ending between June 1, 2000, and May 31, 2001. Depending on where in this time period a company's fiscal year ended, some call it fiscal year 2000, others fiscal year 2001. In last year's scorecard, we reported the figures as belonging solely to fiscal year 2000. In reality, the figures (covering fiscal years ending between June 1, 1999, and May 31, 2000) tracked what some companies indeed called fiscal year 2000 but many termed fiscal year 1999. This year, to avoid any confusion caused by labeling the columns with a specific year, we chose to categorize our figures as "Latest Year R&D Spending."

		R&D SPENDING (IN MILLIONS)			REVENUE (IN MILLIONS)		R&D SPENDING AS % OF REVENUE		NUMBER OF EMPLOYEES	R&D SPENDING PER EMPLOYEE (IN DOLLARS)	
	COMPANY	LATEST YEAR*	RANK	% CHANGE FROM PREVIOUS YEAR††	LATEST YEAR*	% CHANGE FROM PREVIOUS YEAR	LATEST YEAR*	RANK	LATEST YEAR*	LATEST YEAR*	RANK
AEROSPACE	BAE Systems (U.K.)	2,181	1	72.6	13,996	37.0	15.6	1	85,000	25,656	1
	Boeing (U.S.)	1,998	2	49.0	51,321	-11.5	3.9	5	198,000	10,091	3
	United Technologies (U.S.)	1,302	3	0.8	26,583	10.2	4.9	4	153,800	8,466	4
	Honeywell International (U.S.)	818	4	-10.0	25,023	5.4	3.3	6	125,000	6,544	6
	Rolls-Royce (U.K.)	538	5	72.6	8,508	23.6	6.3	2	46,600	11,551	2
	Raytheon (U.S.)	526	6	3.5	16,895	-1.8	3.1	7	93,700	5,614	7
	Thales† (France)	375	7	0.6	6,149	11.6	6.1	3	48,920	7,673	5
AUTOMOTIVE	Ford Motor (U.S.)	6,800	1	-4.2	170,064	5.9	4.0	8	345,991	19,654	2
	General Motors (U.S.)	6,600	2	-2.9	184,632	4.6	3.6	11	386,000	17,098	4
	DaimlerChrysler (Germany)	5,656	3	10.5	144,922	8.3	3.9	9	416,501	13,579	6
	Toyota Motor† (Japan)	3,969	4	-7.0	112,751	1.0	3.5	12	210,709	18,836	3
	Volkswagen† (Germany)	3,381	5	25.6	67,084	9.5	5.0	6	306,275	11,039	7
	Honda (Japan)	3,089	6	5.6	56,586	6.0	5.5	5	114,300	27,023	1
	Bosch (Germany)	1,812	7	5.7	28,162	13.1	6.4	2	198,666	9,121	9
	Delphi Automotive Systems (U.S.)	1,751	8	3.0	29,139	-0.2	6.0	4	211,000	8,299	10
	Renault† (France)	1,596	9	15.1	33,550	1.1	4.8	7	159,608	9,997	8
	Denso† (Japan)	1,401	10	—	16,488	7.1	8.5	1	—	—	—
	Peugeot† (France)	1,300	11	12.0	33,741	12.0	3.9	9	165,800	7,843	11
	Visteon (U.S.)	1,198	12	7.4	19,467	0.5	6.2	3	82,000	14,610	5
BIOTECH	Amgen (U.S.)	875	1	6.4	3,629	8.7	24.1	8	7,300	119,877	5
	Corixa (U.S.)	692	2	768.9	37	39.5	1,870.5	2	538	1,285,522	2
	Genentech (U.S.)	464	3	40.2	1,646	25.5	28.2	7	4,459	104,097	6
	Genzyme (U.S.)	380	4	143.6	903	17.0	42.1	4	4,400	86,345	7
	Curis (U.S.)	321	5	2,972.2	1	-68.1	31,306.8	1	136	2,357,220	1
	Biogen (U.S.)	303	6	36.9	926	16.6	32.7	6	1,475	205,315	3
	Chiron (U.S.)	293	7	15.5	888	16.4	33.0	5	3,422	85,605	8
	Applera (U.S.)	275	8	53.3	1,371	12.7	20.0	10	4,868	56,449	10
	Millennium Pharmaceuticals (U.S.)	269	9	68.1	196	6.9	136.9	3	1,330	202,060	4
	Serono (Switzerland)	263	10	18.7	1,147	8.8	22.9	9	4,268	61,657	9
CHEMICALS	Bayer (Germany)	2,126	1	11.3	26,762	19.0	7.9	3	122,100	17,411	6
	DuPont† (U.S.)	1,765	2	-54.4	28,268	5.0	6.2	4	93,000	18,978	4
	BASF (Germany)	1,362	3	14.5	32,080	22.0	4.2	7	103,273	13,186	9
	Dow Chemical (U.S.)	898	4	5.5	23,008	15.1	3.9	9	41,943	21,410	3
	Akzo Nobel (Netherlands)	705	5	8.8	12,497	-3.0	5.6	6	68,400	10,308	10
	Mitsubishi Chemical† (Japan)	583	6	-0.9	14,619	9.0	4.0	8	33,465	17,417	5
	Syngenta (Switzerland)	537	7	—	4,876	—	11.0	1	24,921	21,548	2
	Sumitomo Chemical† (Japan)	520	8	7.8	8,320	2.4	6.2	4	17,474	29,731	1
	EMD (Germany)	487	9	6.2	6,016	26.1	8.1	2	33,520	14,537	8
	Asahi Kasei (Japan)	436	10	30.8	11,113	6.3	3.9	9	26,695	16,321	7
	Degussa† (Germany)	367	11	39.0	11,026	51.9	3.3	11	44,605	8,237	11
COMPUTERS (HARDWARE)	IBM (U.S.)	4,345	1	-5.0	88,396	1.0	4.9	9	316,303	13,737	9
	Fujitsu† (Japan)	3,511	2	1.5	46,005	0.2	7.6	4	—	—	—
	NEC† (Japan)	3,031	3	0.0	43,696	4.9	6.9	5	154,787	19,581	7
	Hewlett-Packard (U.S.)	2,646	4	8.4	48,782	15.1	5.4	8	88,500	29,898	5
	Mitsubishi Electric (Japan)	1,634	5	12.0	36,151	9.4	4.5	13	116,715	14,000	8
	Sun Microsystems (U.S.)	1,630	6	17.8	15,721	33.2	10.4	2	38,900	41,902	2
	Compaq Computer (U.S.)	1,469	7	-11.5	42,383	10.0	3.5	14	70,100	20,956	6
	Xerox (U.S.)	1,071	8	9.4	18,701	-4.4	5.7	7	92,500	11,578	12
	EMC (U.S.)	783	9	36.8	8,873	32.1	8.8	3	24,100	32,497	3
	Ricoh† (Japan)	582	10	-0.4	12,669	1.5	4.6	12	67,349	8,647	14
	Dell Computer (U.S.)	482	11	-0.8	31,888	26.2	1.5	15	40,000	12,050	11
	NCR (U.S.)	401	12	-0.5	5,959	-3.8	6.7	6	32,960	12,166	10
	Apple Computer (U.S.)	380	13	21.0	7,983	30.1	4.8	10	11,728	32,401	4
	Unisys (U.S.)	334	14	-1.7	6,885	-8.7	4.8	10	36,900	9,041	13
	Silicon Graphics (U.S.)	301	15	-20.8	2,331	-15.2	12.9	1	6,726	44,789	1
COMPUTERS (SOFTWARE)	Microsoft (U.S.)	3,775	1	27.1	22,956	16.3	16.4	7	39,100	96,547	2
	Oracle (U.S.)	1,139	2	12.7	10,860	7.2	10.5	9	42,927	26,524	8
	SAP (Germany)	865	3	30.2	5,591	22.6	15.5	8	—	—	—
	Computer Associates International (U.S.)	695	4	-49.0	4,198	-31.2	16.6	6	18,200	38,187	7
	3Com (U.S.)	536	5	-12.3	2,821	-34.9	19.0	4	8,165	65,612	3
	Avaya (U.S.)	468	6	-13.3	7,680	-7.1	6.1	11	31,000	15,097	9
	Automatic Data Processing (U.S.)	460	7	11.6	6,288	13.5	7.3	10	40,000	11,507	10
	Electronic Arts (U.S.)	392	8	50.2	1,322	-6.9	29.6	1	3,500	111,899	1
	PeopleSoft (U.S.)	321	9	7.8	1,736	21.5	18.5	5	8,019	39,969	6
	I2 Technologies (U.S.)	320	10	142.2	1,126	97.2	28.4	2	6,000	53,385	4
	Cadence Design Systems (U.S.)	264	11	20.7	1,280	17.0	20.7	3	5,650	46,804	5
DRUGS/MEDICAL	Pfizer (U.S.)	4,435	1	59.8	29,574	8.0	15.0	7	90,000	49,278	4
	GlaxoSmithKline (U.K.)	3,665	2	99.1	26,231	112.9	14.0	8	108,201	33,873	11
	Aventis (France)	3,105	3	135.9	19,906	77.0	15.6	5	102,489	30,295	14

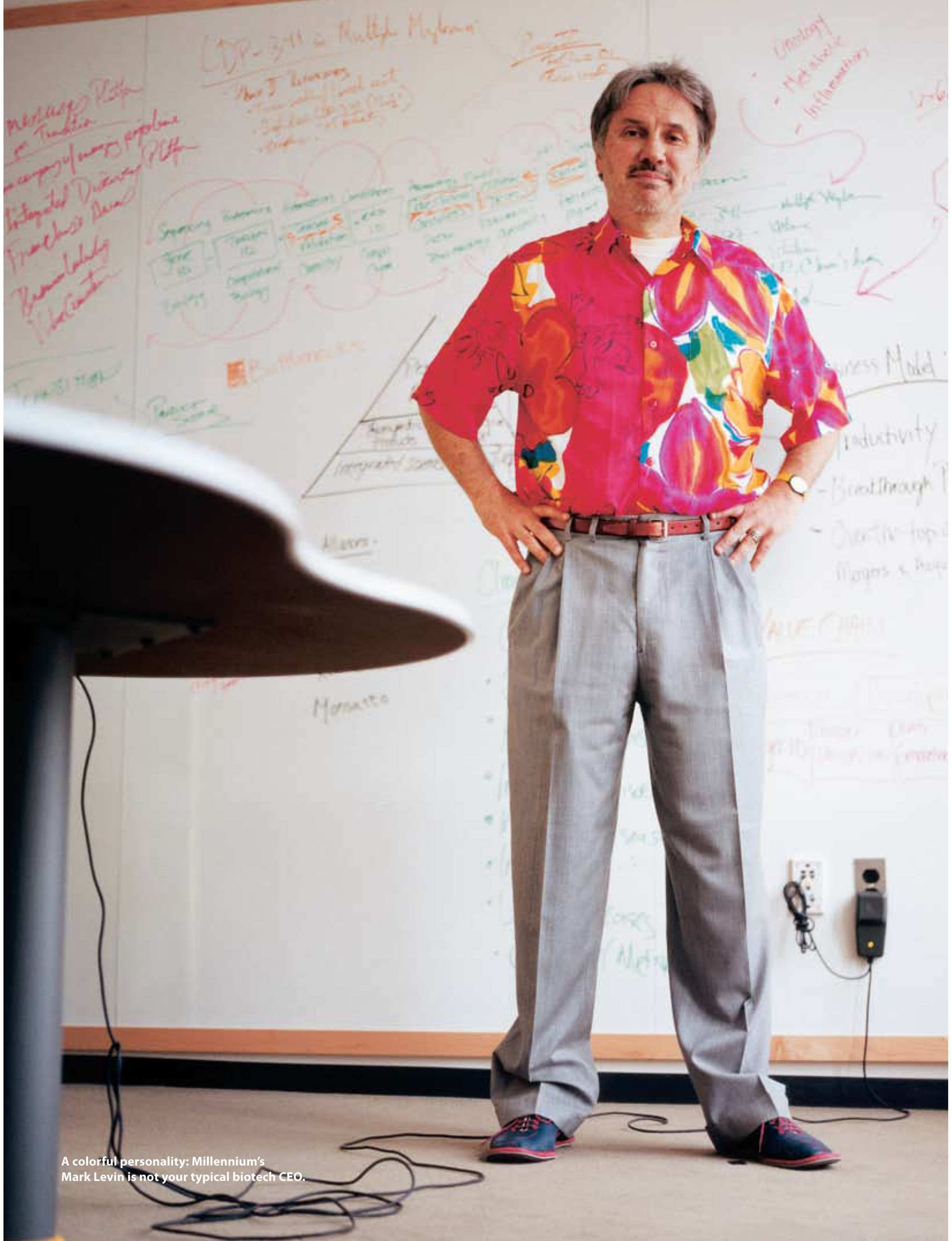
	Johnson and Johnson (U.S.)	2,980	4	14.6	29,139	6.1	10.2	15	98,500	30,254	15
	AstraZeneca (U.K.)	2,893	5	-1.0	18,103	-1.9	16.0	3	57,000	50,754	3
	Pharmacia (U.S.)	2,753	6	113.4	18,144	10.5	15.2	6	59,000	46,661	6
	Novartis (Switzerland)	2,716	7	9.7	20,880	10.3	13.0	11	67,653	40,142	8
	Merck (U.S.)	2,344	8	10.6	40,363	23.4	5.8	19	69,300	33,821	12
	Roche (Switzerland)	2,303	9	4.4	16,720	4.0	13.8	9	64,758	35,570	9
	Eli Lilly (U.S.)	2,019	10	13.2	10,862	8.6	18.6	1	35,700	56,541	2
	Bristol-Myers Squibb (U.S.)	1,939	11	5.2	18,216	7.9	10.6	13	44,000	44,068	7
	American Home Products (U.S.)	1,688	12	-3.0	13,263	11.6	12.7	12	48,036	35,138	10
	Abbott Laboratories (U.S.)	1,351	13	13.2	13,746	4.3	9.8	16	60,571	22,305	17
	Schering-Plough (U.S.)	1,333	14	11.9	9,815	7.7	13.6	10	28,100	47,438	5
	Sanofi-Synthelabo (France)	843	15	3.7	5,322	11.5	15.8	4	29,200	28,883	16
	Schering (Germany)	724	16	18.6	4,010	22.3	18.1	2	23,720	30,514	13
	Takeda Chemical† (Japan)	676	17	-0.3	8,081	9.3	8.4	18	8,025	84,281	1
	Baxter International (U.S.)	665	18	100.3	6,896	8.1	9.6	17	43,000	15,465	19
	Medtronic (U.S.)	578	19	20.4	5,552	10.7	10.4	14	26,050	22,173	18
ELECTRICAL/ELECTRONICS	Siemens (Germany)	4,992	1	6.8	69,966	14.3	7.1	9	447,000	11,167	13
	Motorola (U.S.)	4,769	2	36.1	37,580	13.6	12.7	2	147,000	32,442	4
	Matsushita Electric† (Japan)	4,601	3	5.1	63,901	-4.5	7.2	8	290,448	15,841	10
	Sony (Japan)	3,648	4	5.6	64,036	9.4	5.7	13	181,800	20,066	8
	Philips Electronics (Netherlands)	2,469	5	21.1	33,791	20.4	7.3	7	219,429	11,250	12
	Canon (Japan)	1,703	6	9.3	24,348	6.1	7.0	10	86,673	19,650	9
	Agilent Technologies (U.S.)	1,258	7	26.2	10,773	29.3	11.7	3	47,000	26,766	6
	Sharp† (Japan)	1,080	8	133.9	16,237	6.3	6.6	11	49,748	21,700	7
	Emerson Electric (U.S.)	594	9	16.4	15,545	8.9	3.8	15	123,400	4,813	15
	GEA (Germany)	519	10	—	2,042	31.8	25.4	1	13,889	37,337	2
	Invensys† (U.K.)	438	11	3.1	13,108	-4.0	3.3	16	121,683	3,601	16
	Schneider Electric (France)	423	12	7.0	8,653	15.7	4.9	14	72,144	5,869	14
	Sumitomo Electric (Japan)	392	13	101.1	12,945	13.0	3.0	17	—	—	—
	Qualcomm (U.S.)	340	14	-10.7	3,197	-18.8	10.6	4	6,300	54,033	1
	Tokyo Electronics† (Japan)	325	15	38.3	3,858	40.4	8.4	6	8,946	36,338	3
	Omron† (Japan)	320	16	-13.6	4,862	0.0	6.6	11	24,821	12,910	11
	Teradyne (U.S.)	301	17	31.7	3,044	70.0	9.9	5	10,200	29,502	5
HIGH-TECH CONGLOMERATES	General Electric (U.S.)	1,867	1	12.0	128,487	15.5	1.5	8	313,000	5,965	7
	3M (U.S.)	1,101	2	6.1	16,724	6.2	6.6	2	75,000	14,680	2
	TRW (U.S.)	889	3	-11.5	17,231	1.5	5.2	9	103,000	8,631	6
	Eastman Kodak (U.S.)	784	4	-4.0	13,994	-0.7	5.6	5	78,400	10,000	4
	Fuji Photo Film† (Japan)	715	5	-3.6	12,272	-2.5	5.8	4	37,151	19,258	1
	ABB (Switzerland)	703	6	—	22,967	-6.9	3.1	6	160,818	4,371	8
	Tyco International (Bermuda)	528	7	17.1	28,932	28.6	1.8	7	202,000	2,611	9
	Rockwell International (U.S.)	474	8	12.3	7,151	1.5	6.6	2	41,200	11,505	3
	ITT (U.S.)	391	9	48.0	4,829	4.3	8.1	1	41,553	9,414	5
PETROLEUM	Elf Aquitaine† (France)	577	1	-35.3	31,725	10.2	1.8	2	57,400	10,044	1
	Exxon Mobil (U.S.)	564	2	-10.5	206,083	28.1	0.3	4	—	—	—
	Schlumberger (Netherlands Antilles)	541	3	3.5	9,611	14.5	5.6	1	60,000	9,012	2
	Royal Dutch/Shell† (Netherlands)	505	4	-29.3	105,366	12.5	0.5	3	96,000	5,260	3
	BP (U.K.)	434	5	40.0	148,062	77.2	0.3	4	107,200	4,049	4
SEMICONDUCTORS	Intel (U.S.)	4,006	1	14.4	33,726	14.8	11.9	14	86,100	46,527	8
	Texas Instruments (U.S.)	1,747	2	23.7	11,875	21.7	14.7	9	42,481	41,124	12
	Applied Materials (U.S.)	1,108	3	62.5	9,564	87.7	11.6	15	19,220	57,644	7
	Broadcom (U.S.)	1,049	4	866.1	1,096	110.3	95.7	1	2,706	387,667	1
	STMicroelectronics (Switzerland)	1,026	5	22.8	7,764	54.6	13.2	12	43,000	23,869	15
	Infineon Technologies (Germany)	915	6	38.8	6,499	71.9	14.1	10	27,210	33,632	13
	Advanced Micro Devices (U.S.)	642	7	0.9	4,644	62.5	13.8	11	14,696	43,672	10
	Conexant Systems (U.S.)	630	8	103.3	2,104	45.7	30.0	4	8,800	71,611	5
	LSI Logic (U.S.)	485	9	60.6	2,738	31.0	17.7	7	7,221	67,217	6
	National Semiconductor (U.S.)	436	10	12.8	2,113	-1.3	20.6	5	10,300	42,291	11
	Micron Technology (U.S.)	428	11	32.7	7,336	94.9	5.8	17	18,800	22,739	16
	Analog Devices (U.S.)	401	12	52.8	2,578	77.7	15.5	8	9,100	44,018	9
	Applied Micro Circuits (U.S.)	349	13	962.4	436	152.7	80.0	2	1,169	298,228	2
	Xilinx (U.S.)	299	14	133.7	1,659	62.5	18.0	6	2,678	111,811	4
	Murata† (Japan)	254	15	11.7	4,019	25.1	6.3	16	25,427	9,998	17
	Atmel (U.S.)	252	16	30.0	2,013	51.3	12.5	13	9,091	27,715	14
	PMC-Sierra (U.S.)	249	17	293.6	695	134.9	35.9	3	1,726	144,417	3
TELECOMMUNICATIONS	Nortel Networks (Canada)	5,087	1	47.4	29,910	41.2	17.0	3	94,700	53,716	3
	Lucent Technologies (U.S.)	5,023	2	4.8	33,813	10.4	14.9	5	126,000	39,865	6
	Ericsson (Sweden)	4,264	3	26.6	27,827	27.0	15.3	4	105,129	40,561	5
	Cisco Systems (U.S.)	4,077	4	97.4	18,928	55.5	21.5	2	34,000	119,912	1
	Nippon Telegraph and Telephone† (Japan)	3,067	5	154.4	91,229	7.1	3.4	12	223,954	13,697	11
	Alcatel (France)	2,524	6	34.1	28,031	36.4	9.0	9	131,598	19,179	9
	Nokia (Finland)	2,306	7	47.2	27,110	53.6	8.5	10	60,289	38,251	7
	Matsushita Communication† (Japan)	1,057	8	318.4	8,193	5.0	12.9	6	16,762	63,075	2
	Mannesmann† (Germany)	626	9	14.9	20,763	22.0	3.0	14	130,860	4,781	13
	Corning (U.S.)	540	10	42.8	7,127	50.3	7.6	11	40,300	13,397	12
	France Telecom† (France)	529	11	-22.9	24,305	10.5	2.2	15	174,262	3,038	16
	British Telecommunications† (U.K.)	501	12	28.7	27,154	10.4	1.8	16	132,100	3,789	14
	JDS Uniphase (U.S.)	474	13	99.7	1,430	405.7	33.1	1	19,000	24,953	8
	Alstom† (France)	452	14	-1.7	14,483	15.4	3.1	13	120,700	3,741	15
	Tellabs (U.S.)	415	15	36.7	3,387	45.9	12.3	7	8,643	48,043	4
	AT&T (U.S.)	402	16	-26.9	65,981	5.4	0.6	17	165,600	2,428	17
	ADC Telecommunications (U.S.)	338	17	20.1	3,288	52.8	10.3	8	22,452	15,054	10

*Fiscal year ending between June 1, 2000, and May 31, 2001
†Latest fiscal-year figures were unavailable for this company; figures are from previous year
††May be affected by business acquisitions or divestitures
SOURCE: STANDARD AND POOR'S



We all came over in different ships,
but we're in the same boat now.

Our origins, skin colors or religions may be different,
but our hearts are all in the same place.
Please show tolerance for your fellow Americans.



A colorful personality: Millennium's Mark Levin is not your typical biotech CEO.

PHOTOGRAPHS BY WEBB CHAPPELL

Q & A

CUSTOM-MADE MEDICATIONS

MARK LEVIN, CEO OF MILLENNIUM PHARMACEUTICALS, THINKS MEDICINE IS ABOUT TO BE TRANSFORMED, AND HE HOPES HIS COMPANY WILL HELP MAKE THAT HAPPEN.

With his casual clothes and slightly disheveled hair, Mark Levin doesn't stand out in the scientist-infested Cambridge, MA, neighborhood that's home to his company Millennium Pharmaceuticals. In biotech circles, however, the 51-year-old Millennium CEO and cofounder is known to be somewhat of a character.

First, there's his professional background, which includes not only the typical stints as a drug company biochemical engineer, a manager at Genentech and a venture capitalist, but also forays into brewing and computer sales and marketing. Then there's his uncanny ability to cut lucrative deals for Millennium with big pharmaceutical firms like Bayer and Pfizer, deals that have brought in some $2 billion and that, in some cases, give Millennium 50-50 rights to any drugs developed—arrangements unheard of before Levin hit the scene. And then there are the Halloween parties (Levin reportedly tends to show up in drag) and the CEO's unending fondness for shoes, which he explains this way: "My dad had a bunch of shoe stores, tiny little stores, and so I actually grew up selling shoes. There's nothing I like more than going shoe shopping."

There's an odd parallel between what excites Levin about the men's shoe industry today and his vision for the future of medicine. Just as he lauds the proliferation of shoe styles and colors that lets customers choose a very individualized look, he looks forward to a day when one-size-fits-all drugs will be replaced with a wider variety of treatments, each specially tailored to an individual's illness and genetic makeup. And with a staff of 1,500 and a 2001 R&D budget of $400 million, Millennium is one of the largest companies to throw its weight so decisively behind this idea of "personalized medicine."

Technology Review senior editor Rebecca Zacks spoke with Levin a day after his eight-year-old company's first drug had been approved by the U.S. Food and Drug Administration. Critics note that the anticancer drug did not originate in Millennium's pipeline (the company acquired it when it bought a firm called LeukoSite in 1999). Still, its approval is an important step toward realizing Levin's vision of a "biopharmaceutical" company—a biotech firm that actually produces therapeutic products. Levin's enthusiasm for that vision, as well as his years of experience as a salesman, were plainly evident as he discussed his company, the drug industry and personalized medicine.

TR: What was the idea behind Millennium when you helped launch it?

LEVIN: In the late '80s and early '90s, I was in venture capital and got involved in starting up a lot of companies. I was hearing all this talk about the human genome, so I went out and spent part of my time in Europe and in the States visiting the major genome centers. I took a few years to meet all the people in academia and the industry and to get a sense of what was going on, and two or three key points came out of those discussions. One, the human genome would be sequenced within the next 10 years, so we would know what all the genes are. Even more importantly, people in medicine and science were saying that *all* human diseases had a significant genetic component—back then, that wasn't common knowledge. When you thought about a genetic disorder, you'd think about cystic fibrosis. But we were beginning to realize that obesity and Alzheimer's and cancer and every major human disease had a genetic component. This was the beginning of Millennium—building a technological and biological platform where we could actually get at the cause and pathway of all human disease, as opposed to the symptoms, by understanding the genome.

TR: How was Millennium's strategy different from those of other biotech companies founded around the same time?

LEVIN: Everybody was excited about the genome, but as you might imagine, people thought about it differently. Some formed diagnostic companies by identifying mistakes or [diversity] in genes. Some built companies by compiling genomic information and selling the databases that arose from the information. Others realized that there were going to be important technologies to develop and you could sell these tools and form alliances around them. Millennium was focused from day one on building the biopharmaceutical company for the future by developing personalized therapeutic products.

TR: How has Millennium evolved since?

LEVIN: The vision is very consistent: identifying genes and proteins, thereby understanding the pathways that are involved in the causes of human disease, and developing products that are directly related to the causes. Over the last 10 years, we moved from genes to proteins [targets for drug discovery] to finding small molecules or antibodies that attack the targets, then into animal studies and now into human studies. And last night, we got approval for our first pharmaceutical product [a drug for a certain type of leukemia].

As the company has evolved, our overall strategy has focused on two key concepts. The first one is what we call personalized medicine; it's finding the right target, finding the right drug for that target—and for that person. All of us in the future will be able to go into the doctor's office with our genome on a chip, compare it to the available data on the genetic causes and pathways of different diseases and make decisions with our doctors about preventive and therapeutic medicine. It will tell us what we should be eating and not eating, and the kinds of tests we should be getting. And if we have a particular disease, it will assist us in choosing the best available therapies, based on our genetic makeup.

The second major effort, which is the biggest issue in the pharmaceutical industry today, is productivity. A major pharmaceutical company needs to produce somewhere between three to five new products a year to grow 10 to 15 percent a year. On average, companies produce one or two. So productivity is going to have to double and triple and quadruple over the next few years, or the industry will not survive as it is today. Millennium has put in place a technology platform from gene to patient to increase the productivity of the critical steps.

TR: As you describe it, personalized medicine will involve both tests for genes or proteins that might cause a person problems, and medicines tailored to that person and those genes or proteins. But right now aren't we in a somewhat uncomfortable phase where we have some of the tests, but few of the medicines?

LEVIN: You are right—for the most part the tests have been out there first. But the field is changing rapidly—a new therapy for breast cancer is now personalized to the woman based on her expression of a particular protein. Products that Millennium develops going forward will in most cases have a test and a therapy together. Over the next five to 10 years, we're going to see an explosion of not only these tests, but the integration of tests and therapy for personalized medicine.

TR: Whenever one of these tests comes out, particularly when it's a gene-based test, there are questions about privacy. Is that something you take into consideration?

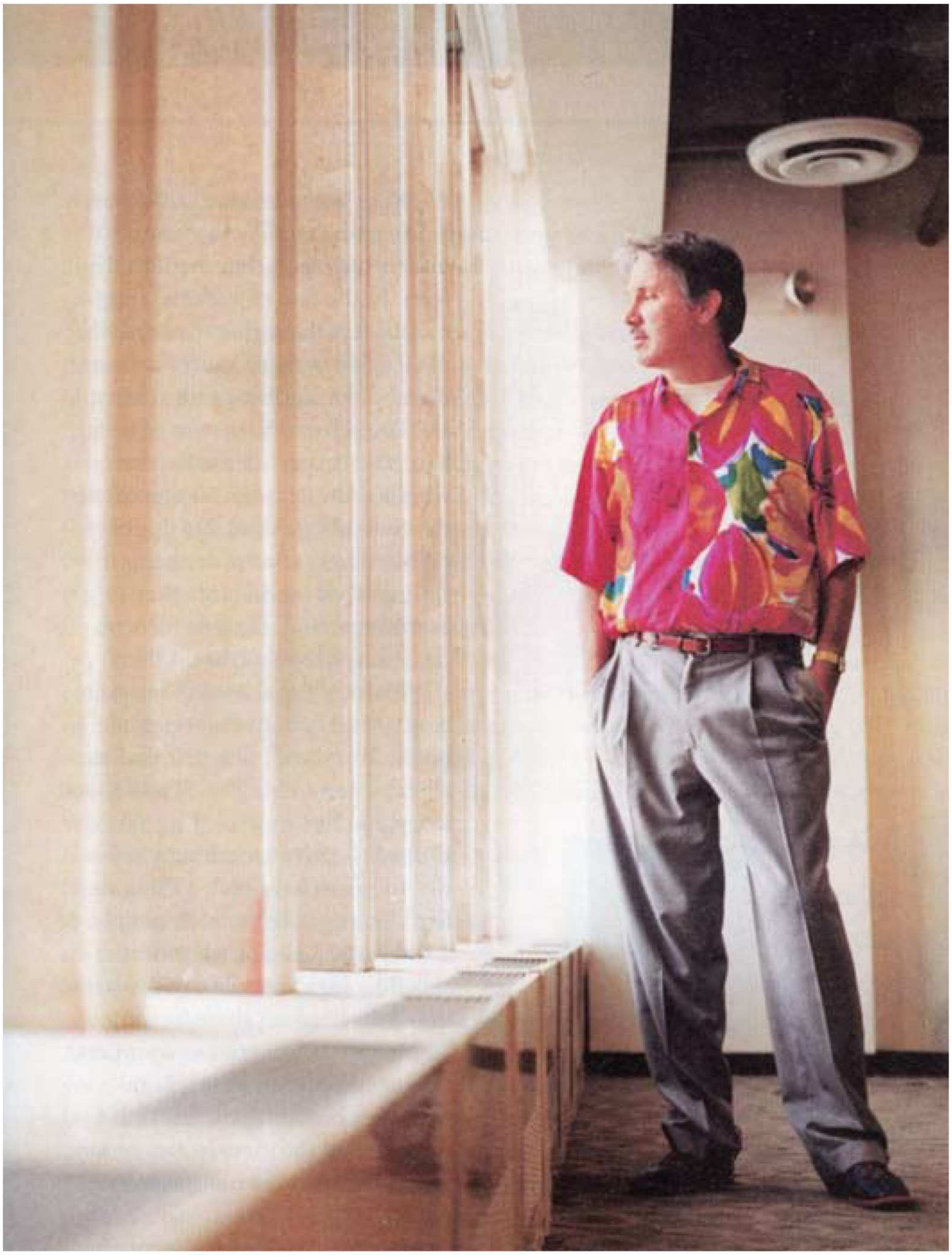
LEVIN: We absolutely do. Our chief business officer, Steve Holtzman [Holtzman has since left that position and acts as an advisor to Levin], was on President Clinton's council for bioethics, and has been very involved in developing policy for the government with regard to privacy. We also recently opened a government relations department in Washington, DC. We believe in order for personalized medicine to be important in the future, one's rights have to be protected.

TR: Does personalized medicine throw a monkey wrench into the economics of drug development? After all, if you're making treatments tailored to patients with a specific genetic profile, aren't you limiting the market for each new drug?

LEVIN: Well, it does and it doesn't. Many products that would have actually failed in the past, because they were toxic on a very small percent of people, will now become very important products for the future because of the ability to determine who should and should not get the drug. Secondly, you're going to get into the clinic and to the marketplace quicker because picking the patient population most likely to benefit for clinical trials will make it easier to prove a drug's efficacy. Thirdly, when we get into the marketplace, products will have more activity and less side effects than today's drugs, thereby being of higher value. And it is also important to remember that when a patient is put on a drug today, 20 to 40 percent of the people are taking a drug that will not work for them.

TR: Are doctors ready for personalized medicine?

LEVIN: It's an important question. If we go back five to 10 years ago and look at the education for doctors, there was almost no training in genetics. Doctors were not getting the kind of training they needed to have a real understanding of how important these technologies are. Today, when you go into medical schools, you see much more integration of genetics and molecular medicine. Every day, we are meeting more doctors in academia and in practice who are very interested and beginning to implement personalized medicine.



TR: You regularly convince the top drug companies to give Millennium what *BusinessWeek* refers to as "obscene amounts of money." How do you do that?

LEVIN: Well, first of all, we don't think they're obscene amounts of money—we think we should have actually gotten more. But what we've done from early on is to tell a vision for the future of the industry that is at the center of not only their profitability but also their survival. Our first alliance was in early 1994 with Roche, and we sat down with Jürgen Drews, who was the president of R&D and who has written a lot about productivity in pharmaceuticals. Right away, Jürgen and the Millennium team came to a real understanding and agreement about what the vision was. As we moved on and talked to other pharmaceutical partners, we found this same understanding about how critical our vision was for the future of genomics, productivity and personalized medicine.

TR: What's in Millennium's pipeline?

LEVIN: We're developing three major businesses today: oncology, inflammation—which includes rheumatoid arthritis and asthma—and metabolic diseases, including obesity and diabetes. We now have seven drugs in the clinic. One of our most exciting drugs in the oncology pipeline is based on inhibiting the proteasome, which is a mechanism responsible for the orderly regulation of proteins and involved in the control of cell growth. We are now [conducting clinical trials of that drug for] multiple myeloma, pancreatic cancer, prostate cancer and many others. We're also developing a molecule with Genentech for inflammatory bowel disease, Crohn's disease and ulcerated colitis; this is an antibody that hones in on T cells that attack the gut. We also have drugs in the clinic for asthma and prostate cancer.

TR: Once you start marketing your own drugs, how does that change your collaborations with the pharmaceutical companies? Are you now the competition?

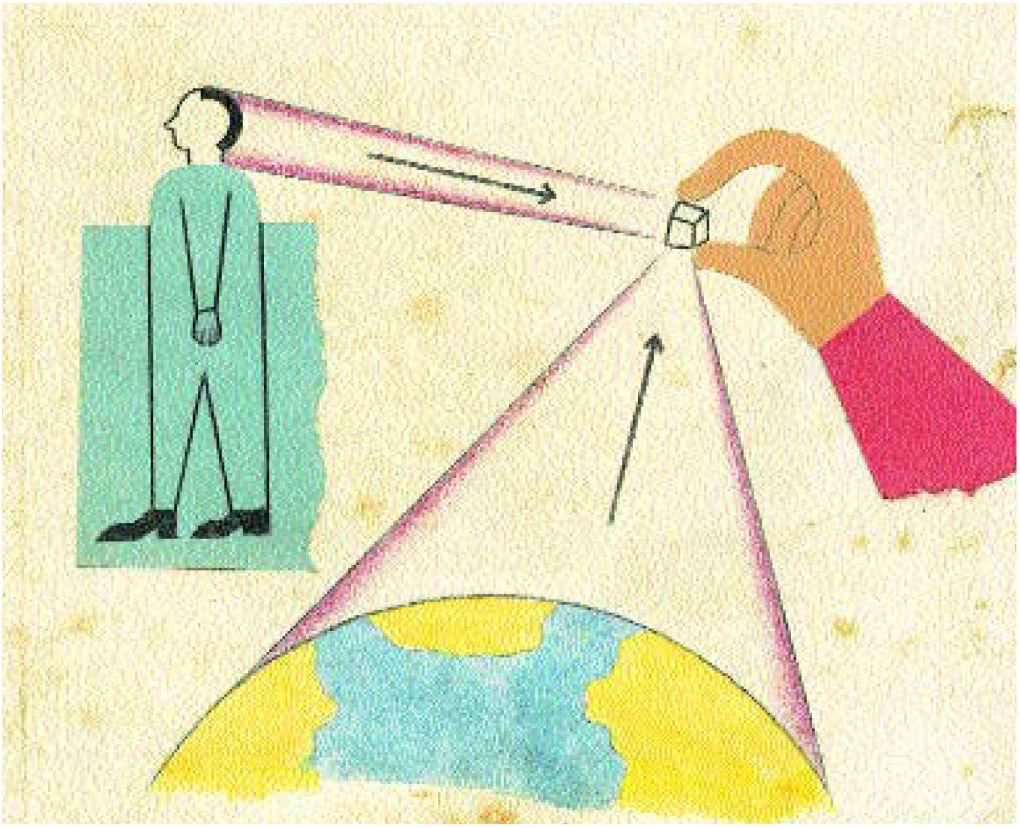
LEVIN: Well, it's certainly been an evolution. Early on, we worked on just genes and drug targets; we would deliver targets to our partners, and we would get royalties on those as they become drugs. Today, we have 50-50 partnerships with Aventis and Abbott Laboratories where we work together to bring drugs from the gene to the market. However, I think it's fair to say that just like pharmaceutical companies see each other as competitors, they are starting to look at us more as competitors. But it's becoming a bigger world: the technologies are more complicated, the biology is more complicated, and in order to do all of this well, you do need to have partners. So although pharmaceutical companies now see us as competitors, they continue to see us as partners.

TR: Has the sequencing of the human genome changed the industry's outlook?

LEVIN: In order to be a successful pharmaceutical company five and 10 years from now, each company's going to have to understand not only the genome but the proteome, have the ability to pick the right targets by understanding molecular medicine, and know how to take the right targets forward into clinical trials. The ability to make those decisions will separate, I believe, the successful companies from the ones that are going to end up being merged into other companies.

TR: What is next for Millennium?

LEVIN: Over the next five to 10 years, our goal is to become a company that's leading the world in personalized medicines, a company that is leading the world in productivity, a company with a value of over $100 billion, a company that has five to 10 products on the market that are making a big difference in people's lives, a company with the strongest pipeline in the entire industry. TR



PHILIPPE WEISBECKER

LIVING MEMORIES

Our tiny dive boat bobs on the crystal blue Flores Sea, about a mile from the primitive Indonesian villages along the shore. I tighten my fins, swig a few test gulps of air through my scuba gear and am about to roll in. Suddenly, a black beast the size of a minivan explodes out of the water. The enormous splash rocks the boat. “Manta ray,” our divemaster says. “They’re showing off. Like puppies. Okay. Now you, jump in.”

Underwater, no one can see you sweat. I shrug, roll into the water and descend through schools of neon and Technicolor reef fish into the coral jungle. The weird growths, the psychedelic formations—giant corals, some like moose antlers, some flaming red with spikes, some like brains—make for a surreal scene. It’s like swimming into a Dalí painting.

I float over to a couple of big groupers. They’re the size of large dogs. As I watch, three or four miniature, delicate “cleaner” shrimp hop fearlessly into the mouth and gills of the first fish, who waits politely for his cleaning. It’s a little like a car wash. Then there’s the boxer crab, whose front claws appear clad in big white boxing gloves—which turn out to be two fluffy white sea anemones. The crab carries these poisonous creatures constantly, jabbing them at prey like an aquatic Muhammad Ali.

Even the most seasoned divers are overwhelmed by the parade of bizarre life forms that dwell in the reefs. In the face of such dazzling beauty, it is shattering to realize that the world’s coral paradises are perishing at an alarming rate. Almost 100,000 square kilometers of reefs have died; experts estimate that within a few decades, 60 percent of the reefs will be dead. No doubt, extraordinary species are being extinguished even before they’ve been discovered. It made me wonder: who’s keeping tabs on this?

Many of the animals I saw were easy to find later in the reef guidebooks. But some I couldn’t find at all. How would I know if I had found a new species? And what would I do if I had? Is there an institute in Sweden to call to have such a thing verified? Do they need a DNA sample, or a whole specimen or what? Professional biologists would know what to do—but shouldn’t there be some way to tap the energies of countless amateurs? After all, the search to comprehend the natural order didn’t begin or end with Carolus Linnaeus, the 18th-century Swedish botanist who devised the modern taxonomic system of identifying life forms; weekend naturalists have much to add to communal knowledge.

Naturally, the Internet is where much of this is happening. The National Biological Information Infrastructure (www.nbii.gov), for example, knits together the biological databases of hundreds of companies, universities and government agencies. At the grass-roots level, the Tree of Life at the University of Arizona (phylogeny.arizona.edu/tree/phylogeny.html) exemplifies the amateur and academic urge to classify. It’s a community-authored phylogeny of earth’s life forms. So if you did find a strange fish, you could probably uncover an avenue online for reporting it.

But an even more remarkable effort is just beginning. Amid this taxonomic flurry, something quite fundamental is strikingly missing: the genes. That’s where the new All Species Foundation comes in. Founded last year, the foundation aims to record all of the earth’s genetic information. Its manifesto (www.all-species.org) begins, “If we discovered life on another planet, the first thing we’d do is conduct a systematic inventory of those life forms. This is something we have never done on our home planet.” The organization’s goal: “Within the span of our own generation, record and genetically sample every living species on earth.” In other

words, build a comprehensive DNA zoo. Accomplishing this will require massive philanthropic input, new biotech tools and the observational powers of a vast population of weekend naturalists.

I learned of this foundation from board member Stewart Brand, of *Whole Earth Catalog* fame, who has yet again placed himself at the epicenter of a seminal infotech movement. And like many of the loftiest scientific undertakings—sequence the genome, put a man on the moon—this one is so audacious that it seems almost daft to attempt it. Yet there is so much that must be learned. Biologists estimate that only about a tenth of earth's species are formally known to science. Maybe it's just a hundredth. At the rate we're going, many species will be extinct before they're even discovered.

The All Species folks aren't just accumulating a massive collection of beetles. It's the DNA they're after: the core record of life on earth. Sequencing the human genome was just a small step for man. University of Texas at Austin biology professor David Hillis quipped that after the All Species work succeeds in 50 years or so, biology can become a predictive science. Computers may beat nature at "sim-evolution."

WEBB CHAPPELL

While the Net has become a natural medium for sorting out nature, what will sort out the Net? That's the mission of an equally audacious project called the Internet Archive (www.archive.org), launched several years ago by Brewster Kahle. Before most others, Kahle realized that the bits people were flinging online could be bottled up and archived.

This isn't as crazy an idea as it might seem. Think of the problem personally. Everything you utter in a year amounts to about four gigabytes of digitized speech. That's half a DVD disc, or four postage-stamp-sized memory chips. In another 50 years, say, a lifetime of spoken output will fit in one of those sugar-cube-sized terabyte stores that surely are coming. This dramatically changes the way we think about the record of our lives, as individuals and societies. The roughly 18 million books in the Library of Congress add up to about 18 terabytes—less than $40,000 worth of disks at today's prices. This means that the Web—which is now the de facto sieve for capturing social output—may be, though evanescent, containable.

When he established the Internet Archive, Kahle acquired a building in an old army barracks in San Francisco; he envisioned the archive as something of a national park for bits. Now, much of the Web is contained in a bay of hard drives in the basement. "It's a Sisyphean task," says Kahle. As they pushed the boulder up the hill, the archivers thought, Since Web pages change over time, why not record with that in mind? So recently, they've built a "Wayback Machine": a browser that lets you set the time. If you want to surf the Web as it was back in, say, 1996, just turn the dial.

Why do these efforts matter? Few things are more precious than the record of experience, whether it's distilled in a journal or encoded into DNA by evolution.

Consider horrific extinctions. When marauding empires want to kill a culture, they cut out its heart. The Romans sacked and burned Alexandria. The Nazis burned books and people. The Khmer Rouge murdered teachers and artists, obliterating the cultural soul of its country. Al-Qaeda stabbed at the heart of modern capitalism—the World Trade Center. Shortly after the buildings imploded, office papers fluttered into the gutters of Brooklyn, miles away. Undoubtedly many companies, running close to the bone, couldn't afford to safely clone their archives in more than one place. Those companies are out of the corporate gene pool forever. Even when people are fortunate enough to survive, the irrevocable loss of institutional memory, as recorded on paper and disks, makes rebooting a business impossible. Fire insurance is nice to have, but if your house burns down, insurance can't restore memories.

Like many of the loftiest scientific undertakings—sequence the genome, put a man on the moon—cataloguing the DNA of all earth's species is so audacious that it seems almost daft to attempt it.

If the surge in computer development has taught us anything, it's that computer memory is so cheap and getting cheaper, so large and getting larger, that it ought to be considered free and infinite. And in a sense, the Internet makes transmission free, too. For the same reason a diffuse network can survive all but the most massively widespread catastrophes, diffuse memories cannot be extinguished. A little like DNA, the bits reside in active vessels and can be transmitted into the future.

Human beings survive as a species because we flock together. After a tragedy, families and communities draw closer. We reach out and hold onto each other. This is why we touch, and why we love. For the same instinctive reason, we gather our memories and cherish them. Pools of community memory gain depth and power over lifetimes. They allow us to reflect, to project and to carry our understanding beyond the here and the now. If you believe that earth's living memories should live on—both the human record and the natural record—then you have to believe that efforts like the All Species Foundation and the Internet Archive really matter. But it is still a shock to many that such intrepid enterprises have scarcely begun.

This is my last column for *Technology Review.* The fledgling process of archiving global life and human thought is a profoundly important note to end on. The world is being transformed by technology, more radically now than ever, and it has been a pleasure to share my thoughts on things that matter.

VISUALIZE

HOW TECHNOLOGY WORKS

COURTESY OF PANASONIC

PLASMA DISPLAYS

Individual cells of xenon gas produce great pictures

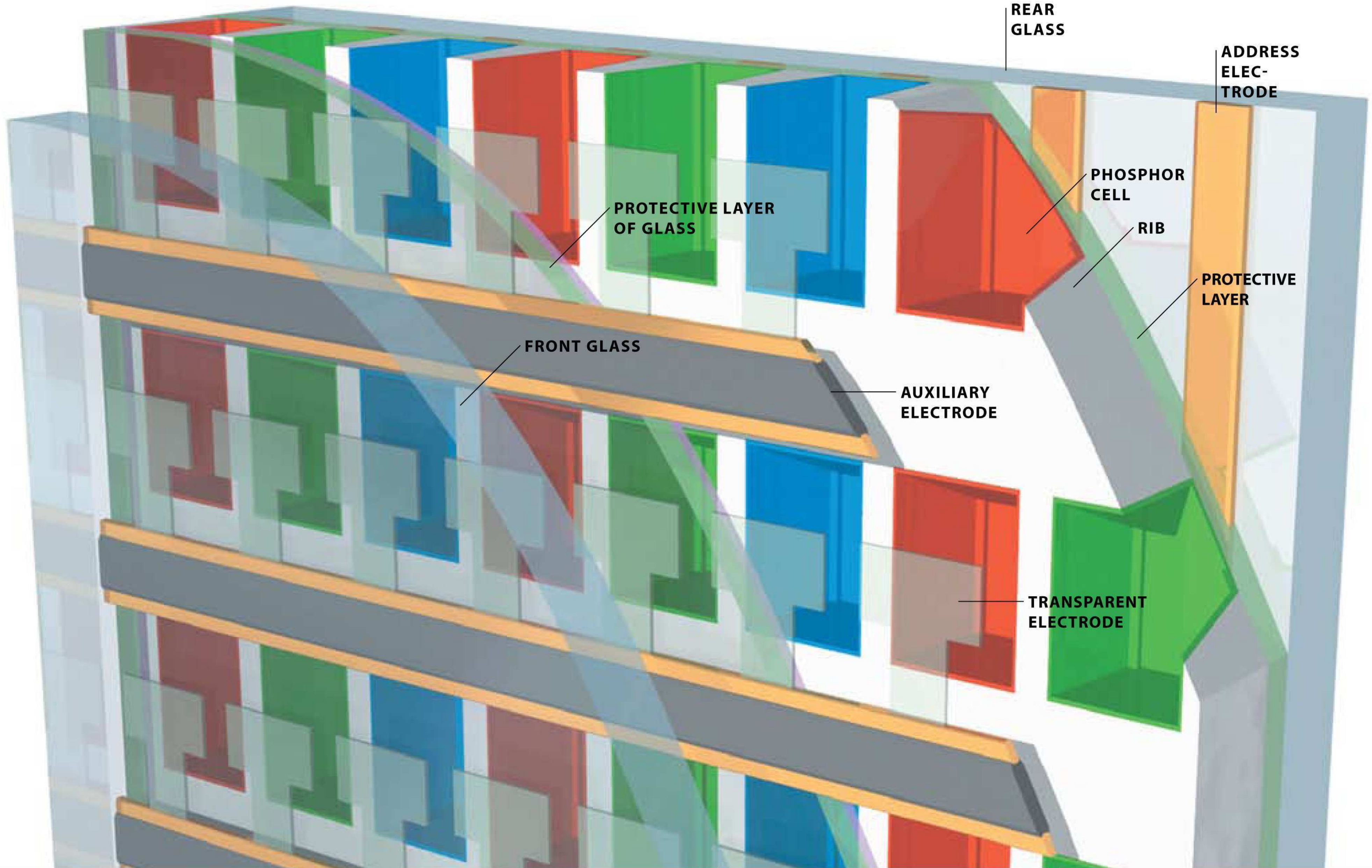
BY TRACY STAEDTER | ILLUSTRATION BY JOHN MACNEILL

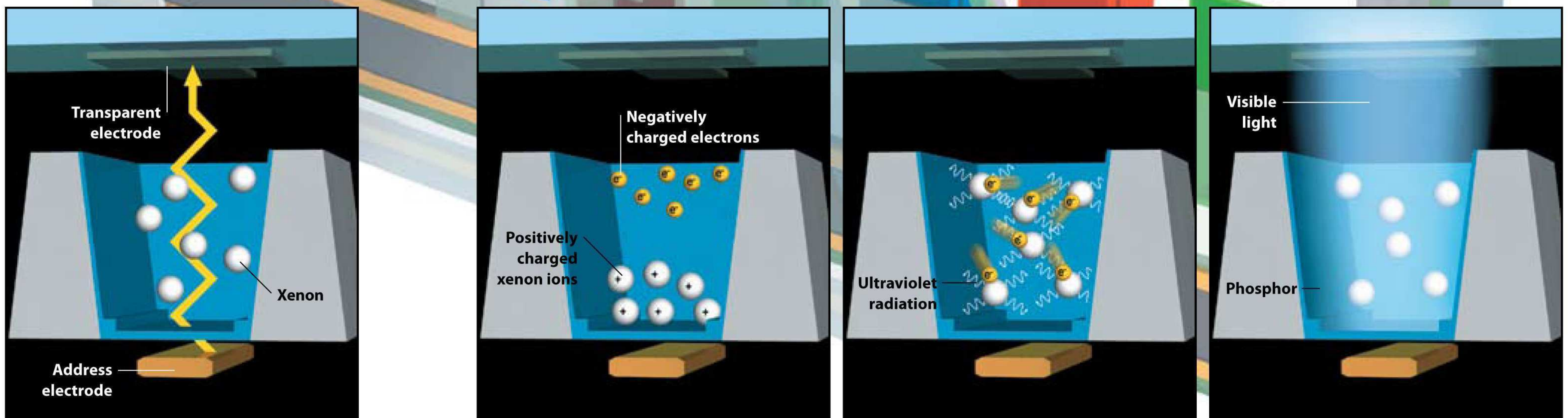
Plasma displays are wide enough, thin enough and light enough to hang on the wall as art. And though consumers have historically been reluctant to dole out the $15,000 to $25,000 it takes to buy a 127- to 160-centimeter unit, prices are starting to fall. Fujitsu Hitachi Plasma Display (a joint venture between the two Japanese giants) recently announced it would begin selling 81- and 94-centimeter versions for $4,500—not cheap, but not far from the price of top-of-the-line projection TVs used for home theater systems.

The sources of such high-quality images are hundreds of thousands of tiny, xenon-gas-filled cells sandwiched between two layers of glass embedded with rows of electrodes. Transparent electrodes in the top layer of glass run perpendicular to address electrodes in the bottom layer. Each cell is lined with either a red, green or blue phosphor, a material that glows when exposed to radiation. Application of an alternating current to two electrodes (via a third auxiliary electrode) produces an electric field in the xenon cell between them. The field energizes the xenon atoms, knocking loose electrons. This creates a plasma, or cloud of electrons and positively charged xenon ions. Within microseconds, some of the electrons fall back into orbit around xenon atoms and relinquish their energy in the form of ultraviolet light. The ultraviolet light strikes the cell's phosphor lining, stimulating it to glow brightly in its characteristic color.

Three cells—one red, one blue and one green—combine to produce one pixel. Different intensities of the three primary colors blend to create more than 16 million different colors—a long way from the 1964 prototype designed by electrical engineers Donald Bitzer and H. Gene Slottow at the University of Illinois at Urbana-Champaign, which projected monochromatic points of orange light and shapes. Because each pixel is illuminated, the image is perfectly focused across the screen, offering viewers a 160-degree viewing angle—instead of the 120-degree angle afforded by projection televisions—and a chance to spread out across the living room for more comfy seats. TR

For an animated version of this illustration, go to www.technologyreview.com/visualize





A voltage applied between the address electrode and the transparent electrode excites xenon atoms in the cell separating them.

Electrons are knocked loose from the xenon atoms, creating a plasma, or a cloud of electrons and ions.

Within microseconds, electrons fall back into their orbits in the xenon atoms and relinquish their energy as ultraviolet radiation.

The ultraviolet radiation excites the phosphor, which emits visible light in its characteristic color (in this case, blue).

A SAFETY NET

Nineteen sixty-two. In the same year as the Cuban missile crisis, the United States Air Force launched a research collaboration with the Rand Corporation designed to provide a reliable system of communication in the case of an enemy attack on North America. Drawing on research at MIT and elsewhere, Rand engineer Paul Baran proposed a packet-switching network that would enable the rapid rerouting of data throughout a decentralized communications system. Baran's instructions were to ensure "minimum essential communications" and thus guarantee "second strike" capability; he proposed an even more robust system allowing contact among *as many as* a hundred networked computers. Baran's proposal was an important landmark in the Internet's prehistory.

September 11, 2001. The attacks on the World Trade Center and the Pentagon launched the first American "war" of the digital age, the first military crisis during which a significant portion of the American public had Net access.

One might well ask, then, how well the Internet functioned as an emergency communications network. In the years since Baran's proposal, the Net has become something larger than what the Rand researchers might have imagined—a vast network linking the civilian population rather than a modest system that ensures data flow between bunkers. "War," for the moment, anyway, means something significantly different as well—a shift from nightmares of nuclear attack to the reality of terrorist actions. And the communications that have turned out to be the most essential in the wake of those actions are not those aimed at coordinating a swift military strike, but rather those that express the loss and fear of the civilian population.

From a purely technical perspective, the system worked better than anyone might have anticipated. While the World Trade Center housed an important relay system for cell phones, and its destruction thus left many New Yorkers without telecommunications, there was no significant national disruption of the computer networks. In the hour following the attacks, many national news Web sites were swamped by a sudden surge in traffic. But within a few hours, they had stripped down their front pages and expanded the number of mirror sites. And the Net itself never faltered. Countless e-mails—in many cases, final messages—were sent from the World Trade Center when the victims of the attack were unable to reach their loved ones by telephone, and many more were sent by people around the country seeking any kind of information about friends or family who were unaccounted for following the buildings' collapse.

Americans returned to network television in the days following the tragedy, reassured by the familiar voices of the news anchors, overwhelmed by the repeated images of the airplane striking the second tower, engulfed in expressions of nationalism. The networks offered nonstop coverage without commercial interruption for more than 90 hours, the longest single block of news coverage in the history of American broadcasting, and viewership was at a record high. Yet the Net and the Web served personal needs that these more public channels of information could never touch.

In recent years, some have expressed doubt that online communities are real communities with hearts and souls. They surely would not have expected the enormous outpouring of grief and caring that flowed through the Internet in the days following September 11. My colleagues describe how their friends and families began to circulate poetry as part of the process of coping with their feelings of powerlessness and anxiety. Net groups reached out to their members in New York and Washington, DC, or found themselves confronting feelings of enormous loss over the deaths of people they had only met online and never knew face to face. Fan discussion lists organized to donate blood or otherwise support the relief efforts. In my own case, my e-mail to my parents was recirculated to more distant family members or people in their church community.

The Twin Towers fell, but the Internet didn't falter. First envisioned as an emergency communications system for the military, the Net turned out to be invaluable for shocked, grief-stricken civilians.

And in this manner, messages—both profound and trivial—flowed from one enclave to another. Intellectuals sent analyses, churches prayers, militants hate mail, pacifists cries for peace and companies spam. Netscape demonstrated the reductive click-here menu-driven triviality of commercial interactivity, asking respondents to decide whether they felt sad, shocked or angry at what had occurred. We may never know how many people received the insightful words of Afghan-American author Tamim Ansary, who warned us that we could not bomb his homeland back to the Stone Age, because after decades of occupation it was already there, or the rather distasteful parody of bin Laden set to the verse of Doctor Seuss's *How the Grinch Stole Christmas.* Despite the seeming exhaustiveness of the television newscasts, many used the Web to read foreign coverage and thus gain a better perspective on the United States' position in the world. Many circulated petitions or words of protest or calls to arms, returning to an ideal of grass-roots democratic participation which stands in stark contrast to the ideas about military authority and elite decision-making that shaped the original Rand studies.

This was a new kind of national crisis and it demanded a new kind of emergency communications system. What Americans needed was a safety net, not an information superhighway. I think they found it was already there. TR

WEBB CHAPPELL

INDEX

PEOPLE AND ORGANIZATIONS MENTIONED IN THIS ISSUE

▸ SUBSCRIBER SERVICES

BILLING QUESTIONS, ADDRESS CHANGES, GIFT ORDERS OR SUBSCRIPTION INQUIRIES:
Technology Review
Subscription Services
PO Box 420235
Palm Coast, FL 32142-0235
800-877-5230

INTERNATIONAL CUSTOMER SERVICE:
386-447-6352

ADDRESS CHANGES:
www.technologyreview.com/custserv/addresschange

INQUIRIES:
www.technologyreview.com/custserv/inquiry

AN MIT ENTERPRISE TECHNOLOGY REVIEW

BACK ISSUES
To order a back issue, please visit our Web site at **www.technologyreview.com/custserv/backissue**. Or send a check or money order for $6.50 to *Technology Review* Back Issues Dept., PO Box 420235, Palm Coast, FL 32142-0235.

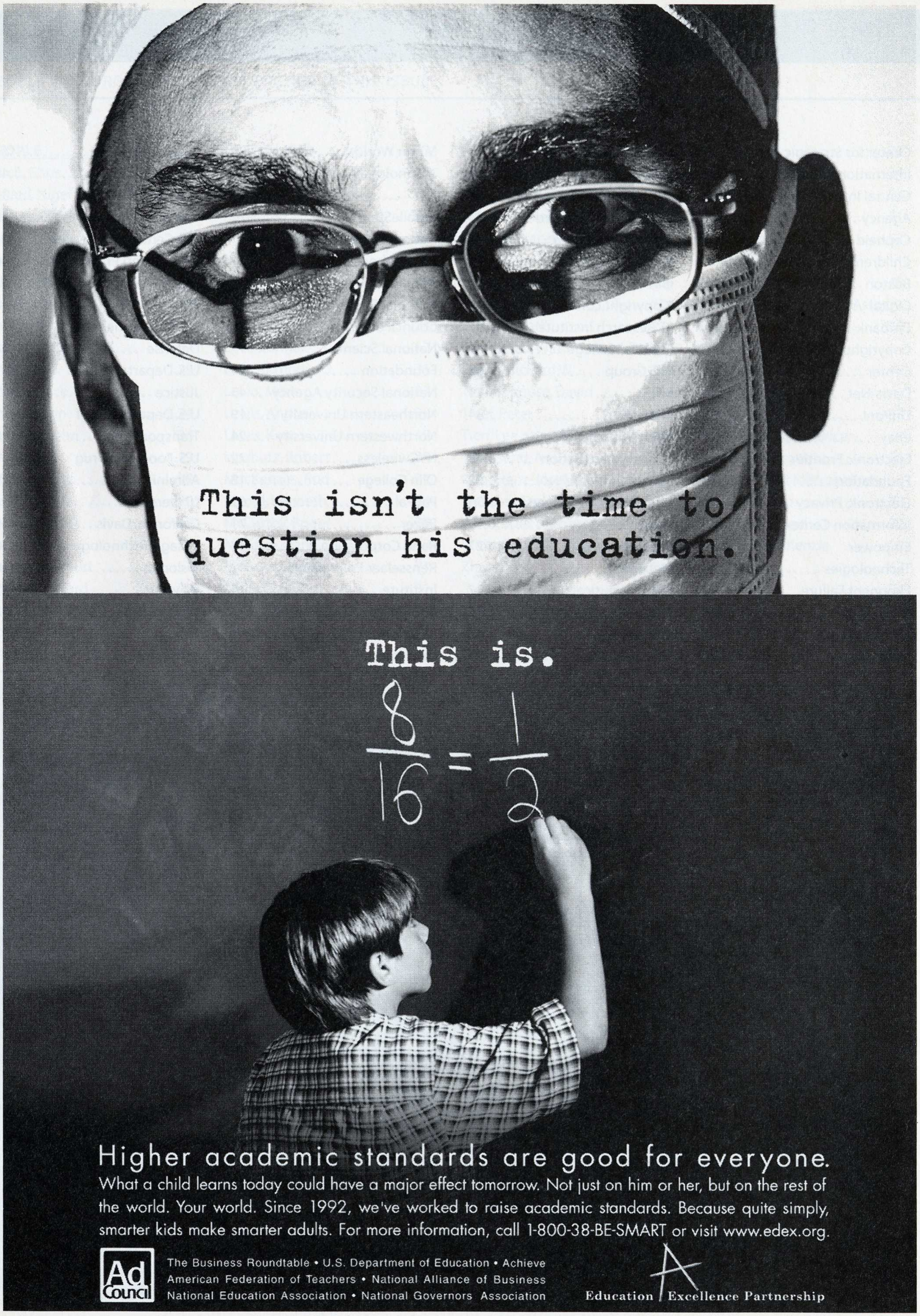
ARTICLE REPRINTS (100 OR MORE)
Contact Reprint Management Services at 717-399-1900, sales@rmsreprints.com or **www.rmsreprints.com**.

PERMISSION TO PHOTOCOPY
Contact Copyright Clearance Center at 978-750-8400, fax at 978-750-4470, or online at **www.copyright.com.**

PERMISSION TO REPUBLISH
To use an article (text only) or other contents of *Technology Review* in a newsletter, newspaper, brochure, pamphlet, journal, magazine, text or trade book, dissertation, presentation, advertisement, CD-ROM or Web site, please contact Copyright Clearance Center at 978-750-8400, fax at 978-750-4470, or online at **www.copyright.com.**

MISSING OR LATE ISSUES
Technology Review is a monthly publication. As a new subscriber you should receive your first issue 4 weeks after your order is placed. If you are an established customer and your copy of *Technology Review* does not arrive within 4 weeks after an issue date, e-mail, telephone or write us. In either case, we'll get to the bottom of the problem and send you the missed issue. Contact us at **www.technologyreview.com/custserv/inquiry** or call 800-877-5230.

IF YOU MOVE
Send us your old and new address or visit **www.technologyreview.com/custserv/addresschange**. (Please allow 6 weeks processing time.)


This isn't the time to question his education.
This is.
8/16 = 1/2
Higher academic standards are good for everyone.
What a child learns today could have a major effect tomorrow. Not just on him or her, but on the rest of the world. Your world. Since 1992, we've worked to raise academic standards. Because quite simply, smarter kids make smarter adults. For more information, call 1-800-38-BE-SMART or visit www.edex.org.
Ad Council
The Business Roundtable • U.S. Department of Education • Achieve
American Federation of Teachers • National Alliance of Business
National Education Association • National Governors Association
Education Excellence Partnership

CLASSIFIED

CAREERS ADVERTISING
For more information on display advertising in this section, contact:

Kerry Jacobson 561-493-8733
kerry@ovidconsulting.com

Jeff Berube 401-568-7703
jeff@ovidconsulting.com

CLASSIFIED ADVERTISING
For more information on classified advertising, contact:

Amy McLellan 617-475-8005
amy.mclellan@technologyreview.com

Rates are $65 per line with an average of 50 characters and spaces per line. Deadline is 8 weeks before issue date.

THE AUTOAUDITORIUM™ SYSTEM
records auditorium presentations
Automatically, Without A Crew!
Ideal for classes, lectures, seminars
via videotape, telecast, Internet.
www.AutoAuditorium.com

WWW.COMPONENTKITS.COM
We manufacture and sell Electronic Component Kits for engineering design, prototype, University lab, and hobbyists. FREE CD-ROM, newsletter on website.

SMART IS SEXY
Date fellow graduates and faculty of MIT, the Ivies, Seven Sisters and a few others.
The Right Stuff
800-988-5288
www.rightstuffdating.com

Your New Best Friend...

The FREE Consumer Action Website – it's got thousands of links to companies And government agencies – the names, numbers, advice, and connections you need to get your wrongs righted.

Log on to **www.pueblo.gsa.gov,** and click on the FREE Consumer Action Web Site.

www.pueblo.gsa.gov

d

It looks like a perfect d.
The only problem is, it's a p.

It's dyslexia. A reading disability where some kids confuse their d's with their p's, b's and q's. But, with the right help, most of these kids can go on to do well in school. Call 1-888-GR8-MIND or visit www.ldonline.org.

THERE'S NO REASON TO BE HELD BACK.

Ad Council

ccld
coordinated campaign for learning disabilities

Edelman & Associates

is an executive search and technical recruiting firm serving Software, Internet, and other high-technology companies.
Current searches include:

- **Software Configuration Manager**
- **Systems-Level Database Software Engineers**
- **Software Engineers - C++**
- **Technical Architect - Supply Chain Solutions**
- **Embedded Software Development Manager**
- **Imaging Scientist**

Paul Edelman '78

To explore opportunities in confidence, contact
paul@edeltech.com
or call
(508) 947-5300

Visit www.edeltech.com to see searches currently in progress

COURTESY OF JOE OGRODNICK, NEW YORK STATE AGRICULTURAL EXPERIMENT STATION, CORNELL UNIVERSITY

A SHOT IN THE DARK

Genetic projectiles transformed agriculture

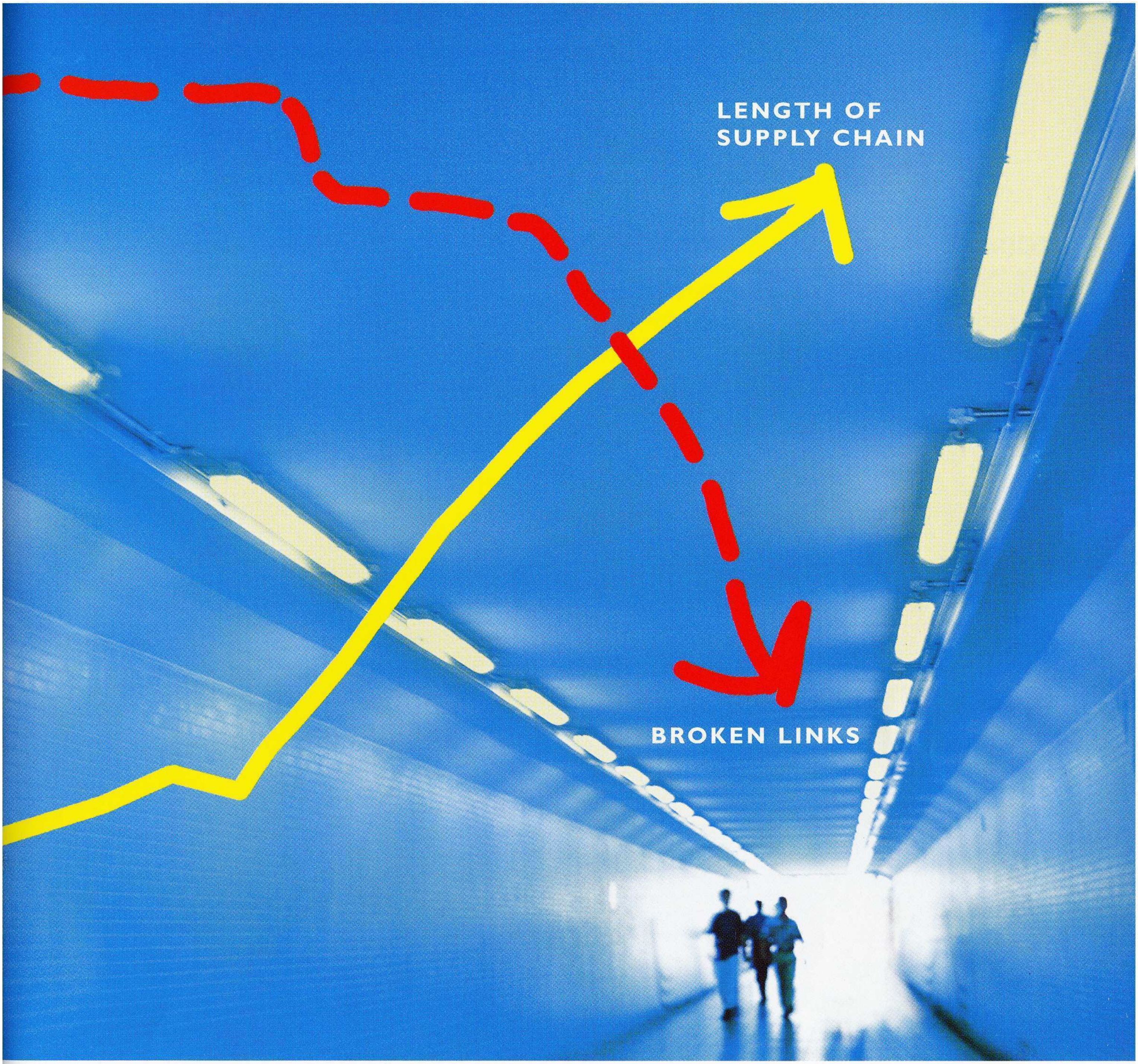
The early days of genetic engineering were pretty crude, especially for plant geneticists. But the technology to insert genes conferring traits like pest resistance into plants has revolutionized modern agriculture. Today a device with origins in a pest reduction battle of a different sort is responsible for virtually all the genetically modified soy and maize crops grown in the United States. It's been dubbed the gene gun.

It all started in 1983, when Cornell University plant breeder John Sanford turned to biotechnology in his hunt for a shortcut past the lengthy and random cross-pollination process commonly used to create new plants. But penetrating a plant's thick cell walls to deliver new genes for specific, desired traits was a challenge. While waging war against a backyard squirrel infestation with a BB gun, Sanford thought of using a similar gun to blast genes through the cell walls. He approached Edward Wolf and Nelson Allen, engineers at Cornell's Nanofabrication Facility, for help designing projectiles to deliver the DNA. The duo decided that microscopic particles of tungsten could be coated with desired genes and shot directly into the cells using a gun. Preliminary tests involved an ordinary air pistol *(above)*.

Theodore Klein, a postdoc in Sanford's lab, tested the scheme on its first subject: an onion. But because the researchers couldn't control the gun's air bursts—the particles either didn't penetrate the cells or destroyed them—early trials frequently left the lab walls splattered with onion bits. Sanford's team then developed a device to use .22-caliber gunpowder charges that provided higher velocities and less shock. In this system, a specially designed plastic bullet charged down the gun barrel, coating itself with the pellets. At the barrel's end, the bullet slammed up against a metal sheet, sending the particles flying at high speed through a small hole in the sheet and into the cells. Within several months, the onion experiments worked. By the mid-1980s, the team had also inserted foreign genes into tobacco, wheat and soybeans.

In 1990, Cornell sold the rights to the technology to DuPont. Since then, "gene guns" have gone through several refinements, making them much more precise. Meanwhile, researchers at Monsanto, Washington University in St. Louis and Ghent University in Belgium developed a competing method using a bacterium to inject DNA into plant cells. Plant geneticists now use both methods with about equal frequency to genetically modify crops. TR

Technology Review (ISSN 1099-274X), Reg. U.S. Patent Office, is published monthly, except bimonthly in January/February and July/August, by the Massachusetts Institute of Technology. Entire contents ©2001. The editors seek diverse views, and authors' opinions do not represent the official policies of their institutions or those of MIT. Printed by Brown Printing Company, Waseca, MN. Periodicals postage paid at Boston, MA, and additional mailing offices. Postmaster: send address changes to *Technology Review*, Subscription Services Dept., P.O. Box 42005, Palm Coast, FL 32164 , or via the Internet at www.technologyreview.com/custserv/inquiry. Basic subscription rates: $34 per year, Canadian residents add $10, other foreign countries add $30. Printed in U.S.A. ABC audited



LENGTH OF
SUPPLY CHAIN
BROKEN LINKS